


3 1761 11648462 7



Digitized by the Internet Archive
in 2023 with funding from
University of Toronto

<https://archive.org/details/31761116484627>



Privacy Commissioner

113

CAI
PC
-AST

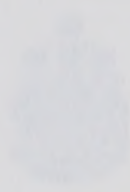
Annual Report 1988-89



Annual Report Privacy Commissioner 1988-89



Annual Report
Privacy Commissioner
1988-89



The Privacy Commissioner of Canada
112 Kent Street
Ottawa, Ontario
K1A 1H3
(613) 995-2410, 1-800-267-0441

© Minister of Supply and Services Canada 1989

Cat. No. IP 30-1/1989

ISBN 0-662-56842-7

“No personal information shall be collected . . . unless it relates directly to an operating program or activity . . .”.

“A government institution shall, wherever possible, collect personal information . . . directly from the individual to whom it relates . . .

“ . . . shall inform any individual . . . of the purpose for which the information is being collected.

“ . . . shall take all reasonable steps to ensure that personal information . . . is as accurate, up-to-date and complete as possible.

“Personal information . . . shall not, without the consent of the individual to whom it relates, be used . . . except

(a) for the purpose for which the information was obtained or compiled . . .”

(or in accordance with specific exceptions set out in section 8)

The Privacy Act

The Honourable Guy Charbonneau
The Speaker
The Senate
Ottawa

June 30, 1989

Dear Mr. Charbonneau:

I have the honour to submit to Parliament my annual report. This report covers the period from April 1, 1988, to March 31, 1989.

Yours sincerely,

A handwritten signature in cursive script that reads "John W. Grace". The signature is written in dark ink and is positioned above the printed name and title.

John W. Grace
Privacy Commissioner

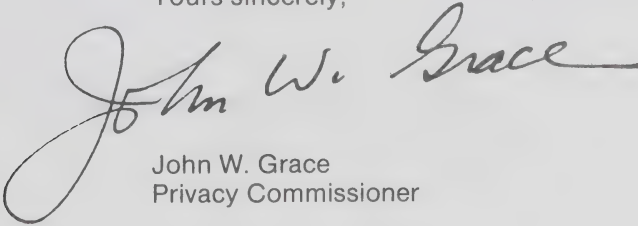
The Honourable John Fraser, P.C., Q.C., M.P.
The Speaker
The House of Commons
Ottawa

June 30, 1989

Dear Mr. Fraser,

I have the honour to submit to Parliament my annual report. This report covers the period from April 1, 1988 to March 31, 1989.

Yours sincerely,

A handwritten signature in cursive script that reads "John W. Grace". The signature is written in dark ink and is positioned above the printed name and title.

John W. Grace
Privacy Commissioner

Contents

Mandate	01
A Mixed Review	02
Who's in Control Here?	10
AIDS and Privacy	14
The Dawn of the Biotechnological Age	16
Computer Security	18
CSIS Files	20
What's with the Cheque?	22
Complaints Directorate	24
Cases	26
Inquiries	38
Compliance Directorate	39
Canada Post	42
Pension Appeals Board	44
Science Council of Canada	44
Department of Finance	45
Ministry of the Solicitor General	46
Employment and Immigration Canada	47
Notifying the Commissioner	50
Spreading the Word	53
Corporate Management	54
Appendices	
I Organization Chart	56
II Government Institutions covered by the Act	57

Mandate

The *Privacy Act* provides individuals with access to their personal information held by the federal government; it protects individuals' privacy by limiting those who may see the information; and it gives individuals some control over the government's collection and use of the information.

The Act sets out the principles of fair information practices, requiring government to:

- collect only the information needed to operate its programs;
- collect the information directly from the individual concerned, whenever possible; and
- tell the individual how it will be used;
- keep the information long enough to ensure an individual access; and
- "take all reasonable steps" to ensure its accuracy and completeness

Individuals in Canada may complain to the Privacy Commissioner if:

- they are denied any part of the information;
- they are denied their request to correct some of the information on the file — or their right to annotate it;
- the department takes longer than the initial 30 days or maximum 60 days to provide the information;
- the Personal Information Index description of the contents of the information bank is deficient in some way;
- the department's listing in the Index does not describe all the uses it makes of personal information;

- an institution is collecting, keeping, using or disposing of personal information in a way which contravenes the *Privacy Act*.

The Privacy Commissioner's investigators examine any file (including those in closed banks) except confidences of the Queen's Privy Council to ensure that government institutions are complying with the Act.

The Act also gives the Privacy Commissioner the power to audit the way government institutions are collecting, using and disposing of personal information.

A Mixed Review

The measure of a year's results in the privacy business can be as variable as the standards used for the calculation. It may even be fraudulent to attempt to sum up the privacy state of the nation with catchy generalizations. The subject is now simply too complex to be reduced to neat themes.

Even the Supreme Court of Canada mixed the results. Here was a year in which the court pronounced in *Her Majesty the Queen v. Brandon Roy Dymnt* that "privacy is essential for the well-being of the individual" and the "restraints imposed on government to pry into the lives of the citizens go to the essence of a democratic state". The message could not be clearer or the source more definitive.

Here the court was re-inforcing its earlier opinion that the protection of "individuals from unjustified intrusions upon their privacy" is established by section 8 of the Charter of Rights and Freedoms ("everyone has the right to be secure against unreasonable search and seizure"). The judgment in the Dymnt case, written by Mr. Justice G. V. La Forest, also set forth the following key principle: "If the privacy of the individual is to be protected, we cannot wait to vindicate it only after it has been violated....Invasions of privacy must be prevented and, where privacy is outweighed by other societal claims, there must be clear rules setting forth the condition in which it can be violated."

The *Privacy Act* is precisely a compendium of such rules. In two cases now, the Supreme Court has given the *Privacy Act* the strongest possible constitutional underpinning, making explicit the application of section 8 of the Charter to privacy protection.

Parliament can take some satisfaction in being ahead of both the Charter and the Supreme Court in having established by the *Privacy Act* the rules to control government uses of personal information collected from its citizens. Parliament is not always thus in advance of the courts in these litigious days.

But the privacy news from the legal front does not bring unalloyed joy. The Supreme Court of Canada's decision in *Stewart v. Her Majesty the Queen* appears to set back the cause. In this case, the court ruled that confidential information cannot be stolen because it cannot be considered property for the purpose of the Criminal Code.

In the case, a union, attempting to form a bargaining unit at a hotel, was unable to obtain the names and addresses of some 600 employees because management treated this information as confidential. A consultant hired by the union obtained the list through a security guard who, for a fee, copied the names from a list on the hotel's premises without removing, or in any way altering, the original document. The consultant was charged under the Criminal Code with counselling to commit fraud, theft and mischief to the private property of the hotel and its employees.

The Ontario Court of Appeal's conviction was overturned by the Supreme Court (in a unanimous decision). Mr. Justice Antonio Lamer wrote for the court that "confidential information is not of a nature such that it can be taken because if one appropriates confidential information without taking a physical object, for example by memorizing or copying information...the alleged owner is not deprived of the uses or possession thereof". The judgment went on to observe that "one cannot be deprived of confidentiality because one cannot own confidentiality".

With great respect, as lawyers ritualistically intone, these observations have alarming implications for the information society in general and the *Privacy Act* in particular. If the *Privacy Act* promises anything, it is the promise of protection for the confidentiality of personal information collected by government institutions. That fine legal point of whether one can own confidentiality is simply irrelevant to the important business of keeping sensitive information confidential.

If this non-lawyerly reading of the court's decision is correct, insufficient weight was given to the significant injury which can occur through unauthorized access to huge amounts of sensitive personal information held by both government and the private sector.

While possible commercial harm seemed uppermost, perhaps exclusively, in the mind of the court, terrible personal tragedy could be the result of the unauthorized disclosures of Royal Canadian Mounted Police investigation records, Canadian Security and Intelligence Service surveillance reports, Health and Welfare medical files — to stay with government.

Yet, the court seems to have said that records could be memorized — or copied (or photographed?) — without any criminal sanctions as long as documents are not physically appropriated.

Stewart v. Her Majesty the Queen did not receive the public attention it deserved. Had the information been sensitive health or financial records and not a mere list of names involved in a commonplace labor dispute, the outcry would have been enormous — and deservedly so.

The *Privacy Act* contains no sanctions. Until this Supreme Court decision, a theft conviction under section 298(1) of the *Criminal Code* or a fraud conviction under section 328(1) seemed deterrent enough. Thus it has seemed unnecessary to argue for a sanction provision in the *Privacy Act*. Now the assumed Criminal Code support has been removed.

True, a breach of trust offence remains. It was the charge successfully prosecuted in the case of the Revenue Canada employee who stole the income tax records of some 16 million persons from a Toronto office of Revenue Canada. However, this offence would not be relevant in situations where confidential personal information is taken by a non-public servant or is elicited by deceit from a public official.

Shortly after the decision was delivered in *Stewart v. Her Majesty the Queen*, the Privacy Commissioner raised his concerns with the then Minister of Justice, the Honourable Ray Hnatyshyn. The Minister felt that, despite the Supreme Court's decision, the *Criminal Code* would continue to deter the improper disclosure of information by public officials. He reiterated the government's commitment to amend the *Privacy Act* to provide a statutory basis for the security standards now contained in the Security Policy of the Government of Canada. The Minister noted 1985 amendments to sections 301.2 and 387(1.1) of the *Criminal Code* which created offences dealing with the integrity of computer systems and services and which protect computerized data including personal information.

However, there continues to be a gap in the law which Parliament should close because significant amounts of personal information are held by government in paper files and since compromise of such information by outsiders cannot be ruled out.

The Supreme Court concluded in *Stewart v. Her Majesty the Queen* that Parliament and not the courts should decide what protection be given to confidential information. Parliament needs to act upon that invitation and protect the integrity of the *Privacy Act*.

In passing that Act, Parliament made an explicit commitment to Canadians that the confidentiality of their personal information held by government would be respected. That is the bedrock upon which this legislation rests. If confidential information can be appropriated with no fear of sanction because "one cannot own confidentiality" then the promise Parliament made in the *Privacy Act* has been, at the least, seriously eroded.

"Owning" confidentiality could be enormously more important than owning physical objects. They, after all, can be replaced. But the loss of privacy is non-renewable. Its loss is nothing less than losing control, a diminishing of human dignity.

Hold the Applause

If it was a good news, bad news privacy year from the Supreme Court, so it was from government. The fairest measure of the government's performance is to test it against its own key commitments and timetable set out in *The Steps Ahead*, which was issued in 1987 in response to the unanimous recommendations of the Justice and Solicitor General Committee. That entirely reassuring document was greeted in this report last year with something of the reverence that the Ten Commandments received at Mount Sinai. When put in place, it was said, the new policies and proposed amendments to the *Privacy Act* would make Canada's third-generation privacy legislation "as good as any in the world".

The government's "plan of action" called for achieving all its goals by the end of 1988. Specific commitments were made: "begin immediately" the process of bringing Crown corporations under the *Privacy Act*; establish the Personal Information Index (the guidebook to the government's holdings of personal information) as a data base and to make it available in machine-readable form. The processes may have begun, but more than a year later these commitments had not been realized.

Other target dates were not met. Directives covering consultation with the Privacy Commissioner on issues with data protection implications were to have been issued by spring, 1988. Amendments to the *Privacy Act*, including the promised statutory basis for information security standards, were to be introduced by the fall of 1988. A public education program on behalf of the *Privacy Act* was to be in place by winter, 1988. Not only were the dates missed, nothing had occurred in these matters as of March 31, 1989.

Of course, these were self-imposed deadlines. Under-estimating implementation difficulties because of over-enthusiasm should not be too much faulted. Besides, some key commitments were made good, if somewhat later than promised. The will to proceed with the unfinished business appears generally strong.

But the sluggishness and the slippages are disappointing.

The next 12 months will demonstrate whether *The Steps Ahead* will be meaningful or largely an empty metaphor. Will the walk in *The Steps Ahead* turn out to be a stroll in the park? In the privacy business today, the Queen's counsel in Lewis Carroll's *Through the Looking Glass* should be the guide:

"Now, *here*, you see, it takes all the running you can do, to keep in the same place. If you want to get somewhere else, you must run at least twice as fast as that".

Two Steps Forward

In last year's annual report, the government was congratulated for making good on two commitments — a new policy controlling the government's own use of the Social Insurance Number (SIN) and new controls on the matching or linking of unrelated data bases. Alas, the government's pace did not match the Privacy Commissioner's enthusiasm. Though the SIN and data matching policies were announced earlier, final approval was given only in April, 1989 — technically outside this reporting year.

Yet, the cliché "better late than never" is appropriate in this case. A year's delay does not take away from the significance of the accomplishment. The data matching controls were described here extensively last year.

The tough new restrictions on the government's own uses of SIN are worth revisiting; they represent the most significant of the major commitments on which the government has made good. The President of the Treasury Board put the issue precisely:

"Many Canadians feel threatened by the use of the Social Insurance Number as a universal identifier. With the rapid development of computer technology, there is a growing concern that the SIN may be misused for linking personal information in ways that may pose a threat to individual privacy".

Thus was announced the "first step by the government" to cap its collection and use of the SIN. A large number of existing uses of the number are to be eliminated over five years and from now on any proposed new collection of the SIN for administrative purposes, other than an existing, approved list, is to be sanctioned by Parliament itself.

The new policy stands up against every natural bureaucratic urge in the public and private sector. It is the first time any government has attempted to roll back the use of its own numerical identifier. Omelettes are more easily and less expensively unscrambled (the estimated cost of \$16 million may be low). But it's being done!

No more will the SIN be a public servant's principal employee number; the armed forces lose the SIN as the military service number. Applicants for permanent residence in Canada will not come with a SIN, nor will applicants for citizenship be required to submit to a SIN.

Commercial fishermen seeking permits, taxpayers applying for fuel tax rebates, candidates for grants and fellowships — all these and others are set free from the usages of the SIN.

It is something of a paradox that an age which has all but lost the concept of sin has so come under the sway of SIN. Babies have been given a SIN as a birth registration number in Prince Edward Island and some funeral directors are said to ask for the SIN of the deceased: thus SIN from cradle to grave; SIN even unto death.

In putting its own house in order, the federal government has new moral as well as legal authority to make good on yet another warning issued to other levels of government and the private sector. Continued mindless and insensitive demands for the SIN invite legislation — and that would be deserved.

...A Step Back

Just three months after the announcement of an enormously encouraging policy to control the SIN, Parliament passed amendments to the *Income Tax Act*, among which required Canadians to disclose their SINs to financial institutions where there had been no such compulsion before. Suddenly, even a bank account couldn't be opened without a SIN.

The new policy was designed to facilitate the reporting of interest income to Revenue Canada, an almost noble purpose. Unfortunately, little or no effort was made to notify the public in advance of the purpose of this new collection and use of SIN.

Despite government's promise to consult the Privacy Commissioner in initiatives affecting privacy, no consultation was undertaken before the legislation was introduced. The efficiency of tax collection was accepted by the government as justifying a new use of the SIN without any apparent consideration of the inherent privacy dangers.

In the complexity and detail of the amendments to the *Income Tax Act*, the extension of the SIN and its significance was missed by members of Parliament, the media and, yes, the Privacy Commissioner's Office. One simply did not expect such legislation to contain anything of interest to the business of privacy protection. Of course, the fact that it did demonstrates the vulnerability of privacy to assault from the most unexpected quarters.

The provisions in the new *Income Tax Act* amendments have, for the first time, made it a punishable offence to refuse to provide a SIN. Government institutions have had by statute and regulation the authority to demand SINs, mainly for such social programs as unemployment insurance and pensions. (No number, no coverage, no benefits). Now, no number and a \$100 fine. (What happens for refusing to pay the fine is not clear. Two days in jail?)

Another precedent is established here. Until these income tax amendments, Canadians were required by law to give their SINs only to the federal government. Now they must confess their SINs to banks, trust companies, stock-brokers, credit unions, whenever and wherever they make what looks like an interest-bearing investment. Welcome to the computer society.

Of course, taxes should be paid. There is a relentless consistency in applying the new law once the \$1,000 interest deduction was abolished. But the implications of the new demands for the SIN with the penalty for failure to comply are much more sweeping than anyone appears to have realized. The pity is that no one thought to ask or even to explain.

So soon after announcing the admirable policy to restrict the government's use of the SIN, thousands of private sector institutions (consider the number of bank branches alone!) are authorized to maintain new records systems with the SIN as the identifier. The fact that there is a fine of \$5000 for misusing the SIN is small consolation.

...and Another

In *The Steps Ahead*, the government committed itself to extending the jurisdiction of the *Privacy Act* to cover Crown corporations and their subsidiaries. Such action would almost double the number of institutions covered and, most important, would give visible leadership to the private sector. In implementing the fair information practices, the government was putting its own full house in order.

Since many of these Crown corporations are in direct competition with private sector companies, the coverage by the *Privacy Act* conveys the strong message that the government believes data protection can be a complement, not an obstacle, to good business. Canada Post, after all, has been subject to the legislation for five years and in the face of significant competitive pressures finds that life under the *Privacy Act* does not hinder it commercially.

Though the bulk of the Crown corporations may yet be covered (members of the Privacy Commissioner's Office travelled as part of an awareness task force, meeting representatives of some 21 corporations), two significant omissions, as well as the general delay, have marred the government's initiative.

Neither Air Canada nor Petro-Canada were included on the list of institutions to be brought under the *Privacy Act*.

Air Canada has been exempted because it no longer is a wholly-owned government creature — a dubious ground indeed because the government continues to maintain majority ownership, whatever the future may bring. That itself is reason to hold the government to its original pledge. It would be a dangerous precedent in this age of privatization if mixed ownership were enough to exempt Crown corporations from federal legislation. Until now, it has not. Air Canada itself remains subject to the *Official Languages Act* and, presumably, it would even if it were to be completely privatized. Surely the privacy rights of Air Canada's customers and employees are as important as their linguistic rights.

Other western democracies have recognized the need to bring under data protection codes the vast amount of personal information held in the computers of air carriers. If British Airways can live with the United Kingdom's data protection legislation, Air Canada should be able to live with the *Privacy Act*.

With Petro Canada, ownership is not the issue; Petro Canada is a Crown corporation, pure and simple. But corporation's management has resisted the *Privacy Act* because of perceived difficulties with its operations if it had to live within the Act's principles.

Perhaps Petro Canada's life would be made easier if, for example, the credit files of its customers or lessees did not have to be opened up to those customers or lessees, as they would have to under the *Privacy Act*. Being held exempt from the more onerous demands of human rights or employment equity laws would also make Petro Canada's life easier. But there is no chance of such exemptions. The argument for the legal protection of the privacy rights of Petro Canada's employees and customers is at least as strong.

If such high-profile institutions as Air Canada and Petro Canada were both to be excused from the *Privacy Act*, the government would be rightly viewed as undercutting its own commitments. Almost every institution, public or private, can conjure up reasons to be made exempt from oversight legislation — privacy or otherwise.

Via Rail could object to the *Privacy Act*, so could the Canadian Broadcasting Corporation. Yet both of these institutions (the CBC with some special provisions to protect its news gathering activities) are to be covered.

There may seem to be an air of blissful or naive unreality to a plea to bring two Crown corporations under the *Privacy Act* when the entire private sector, including federally-regulated companies, operates outside the Act. Why worry about Air Canada when other Canadian airlines fly the friendly skies unimpeded by the binding rules of fair information practices? Why insist that the customers of Petro Canada be given the benefits of the *Privacy Act* while those of all its competitors are left to fend for themselves?

Two more institutions in or out of the *Privacy Act* will not make much difference to the overall standard of privacy protection in the country. But if government doesn't insist that its own creatures obey the privacy rules of the road, the private sector is not going to be impressed by preachments to adopt codes such as the data protection principles of the Organization for Economic Co-operation and Development (OECD).

Self Regulation?

All of which raises the effectiveness of the government's effort to encourage private sector firms to respect those OECD guidelines to which Canada is signatory. The Minister of External Affairs' request to major companies to implement these guidelines in their organizations does not appear to have brought any discernible results.

The federal government met on two occasions with provincial governments to develop strategies to encourage the private sector to accept and enforce the guidelines. However, no agreement has apparently been reached as to what business sectors are to be targeted or the strategies to be devised.

The government needs a more vigorous approach. That is the least it can do in light of its rejection of the unanimous recommendation of the Standing Committee on Justice and the Solicitor General that the entire federally-regulated private sector be made subject to the *Privacy Act*.

That recommendation was not accepted (a decision which the Privacy Commissioner supported) because self-regulation seemed to be the preferred way to travel in a time when de-regulation is in fashion. There have been faint stirrings towards self-regulation and there was no evidence of endemic or widespread abuses. Moreover, could a single privacy law be constructed to cover the diversity of the private sector — from banks to cable television companies? Perhaps not. There are practical limits to enforceable regulation in the age of micro-computers. A swollen Privacy Commissioner's Office with brigades of inspectors would give even privacy a bad name.

Self-regulation will be for most, including the Privacy Commissioner, the preferred option to government regulation. Recent "second generation" data protection laws (Ireland, Australia and Japan all adopted legislation within the past 12 months) have been much closer to Canada's model than to the "first generation" laws of Sweden and France which covered the private sector. Without more evidence of effective self regulation, however, the supporters of voluntary data protection codes will be increasingly hard put to defend their position.

Who's in Control Here?

The demands for personal data continue to grow exponentially and unchecked. Arthur Miller, who teaches law at Harvard University, says that his ability to fly depends not on the fact that he is standing at an airport counter waving a ticket. So far as the airline is concerned, unless the right numbers come up on a computer, "I do not exist. I am a mere three-dimensional version of the two-dimensional screen". Let Mr. Miller continue:

"It's not just an airline reservations system. It has my name. It has my telephone number. It has my credit card number. It has who I'm flying with. Whether I've got hotel reservations or a car rental through the system...that's a dossier, and I know it."

And there are more dossiers. Arrive at a hotel and, he says, "you're not going to lay your head down on a Sheraton pillow unless its computer recognizes you. You put it all together and you realize that your life is controlled by one data bank after another, made possible by the computer."

It is a price for convenience and efficiency. No one is suggesting smashing the computers. But ground rules for the handling of the vast amount of personal information being collected should be put in place and respected. Data collections are available, on command, for making the important decisions about us. Arthur Miller is right:

"We have come to understand that it is impossible to get insurance, to get credit, to get certain jobs, get certain government benefits without going through record clearance and record approbation — that people will be looking through our files. Who they are, we don't know. Where they are, we do not know. What the criteria for decision-making might be, we do not know."

We do know (or should!) that information about us in computers can be wrong. But without privacy legislation or working, effective voluntary codes, there is no opportunity to see and correct one's file. Without privacy legislation or enforced codes, there is nothing to stop the frightening growth industry in the sale and exchange of computerized personal information, of data chronicling personal consumption habits (traced through credit card transactions and direct mail orders) and charitable or political contributions.

Who's in control here? Is it individuals of their own information? Or is it personal information collectors and traders with their marvelous machines? To become a "data subject" should not mean becoming any less a human being. Should that ever be conceded, civilization has become subject to its machines and our information societies will have evolved, as Professor David Flaherty of the University of Western Ontario has warned, into "surveillance societies".

Professor Flaherty, an internationally-recognized authority on privacy and data-protection laws, put it in almost apocalyptic terms:

"The various automated data bases now in existence make possible fairly integrated monitoring of individuals in Western countries. The proliferation of such information banks in both the public and private sectors, rather than the existence of any single one of them, poses the fundamental challenge to privacy interests. We need to think about the implications of such surveillance practices for the protection of human rights. In North America in particular, the application of information technology is galloping ahead of regulation and control".

Stripped of one's power to control what the world knows about oneself is demeaning and dehumanizing. There is nothing fringe or dilletantish about claiming privacy rights. They go to the heart of human integrity, of dignity and the kind of society we want. This is why privacy matters.

Privacy matters most of all between citizens and governments because the state has enormous power to extract and use personal information.

Yet, a privacy concordat covering the marketplace is becoming almost as important. Even when personal information is voluntarily given (in many transactions there is precious little voluntariness, e.g., an application for credit), well-defined rules have become essential if individuals are to have at least residual control over the uses of such information.

Some privacy experts, including Professor Flaherty, have come to believe that it is now too late for volunteer privacy concordats in the private sector. They argue that only legislation can control the powerful new technologies and give personal information at least a minimal level of protection. Back to battalions of privacy inspectors and very red bureaucratic tape!

Another privacy scholar, Professor James Rule of the State University of New York, advocated recently that the best way to protect informational privacy is by giving individuals a copyright interest in the commercial use of their own personal data. Information could not be sold or exchanged for value without an individual's permission. An ingenious, fascinating, even logical concept, though highly improbable and unenforceable.

These are desperate solutions, born of frightful visions. Surely there exists a middle way.

The voluntary rules of the privacy road such as the OECD guidelines are entirely sensible and, if implemented, offer some reasonable reassurances. But it has become time for government to treat volunteering in this business much as "volunteers" are traditionally found in the armed forces.

Federally-regulated firms, which the Parliamentary Committee recommended unanimously should be made subject to the *Privacy Act*, would be the place to start. In addition to pursuing more vigorously a cooperative strategy with the provinces to encourage voluntary compliance with the OECD privacy guidelines, the Government of Canada should take on the federally-regulated private sector in a second front of privacy protection activity. Develop effective privacy codes, within a specified time, they should be told, make them known to your customers and employees (who will be delighted!) or, yes, face legislation.

The proponents of privacy laws for the private sector are right about one thing — gentle exhortation has not much worked. But better first to turn the screw a little than impose the heavy apparatus of legislated privacy protection.

Dial Bell for Data

The Privacy Commissioner has not been merely watching these issues from the sidelines, content simply to grade the government's performance. He stepped into the fray upon learning, last November, that the Canadian Radio-Television and Telecommunications Commission was examining whether, to whom and under what conditions, Bell Canada could sell its telephone directory data base of white and yellow page subscriber listings in machine readable form. The initiative was not Bell Canada's but that of companies who have been eyeing Bell's data base with some envy.

This proposal offers chapter and verse on how real the pressure is for the massive exchanges of computerized personal information. At the same time, it is a textbook example of how a sensitive regulatory agency should be alertly aware of the stakes.

In a nice understatement, the CRTC noted that "the provision of this information in machine-readable form may heighten concerns related to customer privacy". "Heighten", indeed! Though nothing is more public than a telephone book, there are good reasons why phone customers should be worried. The Privacy Commissioner put them forward in a formal intervention which asked the CRTC not to require Bell Canada to offer its directories data base to anyone willing to buy.

The reason is this: a qualitative change takes place when names, addresses and phone numbers are moved from paper listings to electronic data processing disks. Special privacy dangers arise because of the infinitely greater accessibility, transmittability and transformability (even the words are ominous) of data in machine readable form. And nothing is closer to home than a telephone book.

One company has already transferred to a 4.7 laser disk the names, addresses and phone numbers of 7.9 million of Canada's 8.5 million households. It was a slow, expensive (more than \$1 million, and this in Pakistan) job.

The phone book was only the start. The same laser disk includes the co-ordinates of each household to within one meter on a grid map of Canada, the names of neighbours, electoral districts, the length of time the occupant has been at that address. Information from 12 demographic fields (sold in aggregated form by Statistics Canada) offers census data as to probabilities of income, language, religion and children. All this is information in the public domain. But add credit card or banking information, if such information was to be made available by fair means or foul, and the result is profiling of the population on a mass, systematic scale.

It is a marketer's dream — a privacy nightmare. Machine-readable listings mean that personal information can be manipulated in any number of creative ways for telephone or mail soliciting. Yet, that would be an almost benign use. Such listings also provide a monitoring or tracking tool of interest not only to marketers but to criminals and, yes, law enforcement agencies alike.

Phone subscribers never dreamed of, much less consented to, this degree of privacy invasion just by the fact of being listed in the telephone directory. Technology makes the danger real and present.

AIDS and Privacy

On another front, and as promised in last year's annual report, the Privacy Commissioner developed recommendations to ensure that AIDS-related personal information is handled by the federal government in accordance with the letter and spirit of the *Privacy Act*. The resulting report, entitled *AIDS and the Privacy Act*, confirms that an appropriate national response to AIDS is perhaps the most sensitive and anguished privacy issue of our time. *AIDS and the Privacy Act* seeks an elusive balance between protecting the privacy of those either with AIDS or infected with the HIV (the virus that causes AIDS), and appropriate disclosures which the protection of others demands.

Compassion towards those afflicted demands that they are protected from the further trauma of unnecessarily invading their private lives and disclosing their condition. The diagnosis of AIDS continues to be a sentence to death. In fact, some current opinion suggests that simply carrying the HIV virus also means early death.

Unthinking and extreme public or government responses to the disclosure of AIDS or HIV infection may, and in some cases have, altered the very conditions of an individual's membership in society: access to schools, work, medical care, even family and friends. That is the simple case to be made for the deepest possible respect for the privacy of the victims.

On the other side, however, disclosure is required, though not nearly as often as is sometimes suggested. Scientific and medical communities may need to know who are the AIDS victims and HIV carriers in the quest to slow, stop or treat the disease. These competing concerns often call for conflicting courses of action.

The report concludes that mandatory HIV antibody testing of such groups as public servants, inmates of federal prisons, immigrants and long-term visitors to Canada, would contravene the *Privacy Act*. The *Privacy Act* prohibits the collection of personal information which is not related directly to a program or activity falling within the statutory mandate of a government institution. Such testing is not a necessary element of any present legislated program.

Of course, Parliament has the authority to override the *Privacy Act* and give government the power to subject groups of individuals to mandatory HIV antibody testing. However, any such action would represent an hysterical over-reaction to the AIDS epidemic — at least so it appears in the present state of knowledge about the disease.

Any public health benefits that would be achieved through large-scale testing are dubious at best and would be far outweighed by the devastating invasion of privacy which would result. Fortunately, privacy interests accord with the most informed medical opinion that AIDS testing should always be voluntary with pre-and post-test counselling.

The Government of Canada has an important leadership role to play in ensuring that AIDS is sensitively handled in the workplace. The report urges Treasury Board, as Canada's largest employer, to issue a comprehensive policy on AIDS in the workplace.

Confidentiality is an integral part of the workplace policy suggested by the World Health Organization. The employee should not be obliged to inform the employer about his or her HIV status, nor is there any need to inform co-workers. If AIDS-related personal information is volunteered, it should be accorded a high degree of protection and, prior to employment, there should be no direct HIV screening (testing) or indirect screening (assessment of risk behaviors or questions about previous tests).

One of the reasons most often given for individuals hesitating to undergo voluntary HIV antibody testing is the fear that they will not be able to control the extent to which third parties will be given access to the information. Indeed, the *Privacy Act* itself sets out some 13 circumstances in which government departments may disclose personal information to third parties without consent. In recognition of the particularly sensitive nature of AIDS information, *AIDS and the Privacy Act* recommends that a tightly controlled process be followed before any such disclosures are made.

Most important, the decision of whether to disclose to third parties without consent should be made only by the head of the government institution. The decision should be based on a consideration of:

1. why disclosure is necessary,
2. the potential adverse consequences of the disclosure on the individual(s) to whom it relates,
3. the likelihood that the requestor can and will maintain the confidentiality of the information, and
4. the likelihood that the requestor will use it only for the purpose for which it was originally sought.

The onus should always be on the requestor to justify the need to release the information without the consent of the individual(s) to whom it relates.

These recommendations attempt to reflect an appropriate compromise between privacy concerns and the legitimate needs of some government institutions. Changes in the understanding of AIDS, its transmission, in public attitudes may compel re-examination of the recommendations as, of course, would a vaccine or cure. In the words of the report:

"To hope for an early cure or an effective vaccine is a natural human response to this terrible disease. But hoping does not diminish society's responsibilities today. The principles set forth here in responding to the privacy issues in handling the personal information of those affected by HIV infection and AIDS may not give much long term comfort. But at least they make society's response more humane. For the moment, perhaps, that is the best we can do."

The Dawn of the Biotechnological Age

By-and-large, the government collects information about individuals in traditional ways, such as by surveys, forms, letters or direct observation. But even these old-fashioned methods can be abused, resulting in unacceptable invasions of privacy. More ominously, however, intrusive collection techniques are gaining currency.

Such methods (some newer than others) permit information about individuals to be drawn directly from their biochemistry: i.e., the breathalyzer and polygraph. Urine tests, blood tests and genetic mapping are also becoming fashionable as means of finding out a person's hidden (perhaps even from himself or herself) secrets.

While these information collection techniques are best known in the law enforcement environment, they are achieving increasing popularity for screening purposes outside of the criminal justice sphere. Would you be a loyal and trustworthy employee? Would you engage in behaviour likely to put others at risk? Have you broken the rules governing an activity in which you want to engage? Do you have a genetic predisposition to certain diseases or personality styles? Governments and private sector employers are being tempted to seek access to biochemistry to provide answers to these questions.

The Department of National Defence, for example, tests the blood of its employees wishing to attend U.S. defence courses to determine if they are HIV free. The Canadian Security Intelligence Service gives prospective employees a polygraph test to determine whether they are loyal and trustworthy. Transport Canada is considering whether transportation workers should have their urine tested for the presence of illegal drugs.

Sports Canada is urging that the urine of funded athletes be tested for the presence of banned (not necessarily illegal) drugs which could enhance performance and undermine fair sporting competition. The RCMP is using genetic material for identification and a national "genetic fingerprint" inventory will be developed similar to that which now exists for fingerprints. Moreover, research is underway into techniques which would enable detailed physical and behavioural profiles to be developed on individuals based on a DNA test.

One commentator has argued that we are moving from the information age into the biotechnological age. In that transition are privacy dangers the likes of which we have not seen in our history.

If privacy is to have any meaning in the 90s and beyond, great care must be taken to ensure that effective limits are placed on new, more intrusive means of information collection. Yet as we end the 80s there are indicators that the policy-makers may not be so inclined.

Some officials testifying at the Dubin Inquiry strongly advocated mandatory, random and unannounced urine testing of federally-funded athletes. While a strong case can be made for such testing, it is troubling that a government policy, even in a well-defined area and with tacit consent of the athletes, appears to ignore a concept which is fundamental to individual privacy — the presumption of innocence. The need to prevent intrusions into private lives, unless there is a specific and reasonable suspicion of wrongdoing, has been clearly articulated by the Supreme Court as part of Canada's Charter of Rights and Freedoms. It has only been compromised in rare instances to protect life — instances such as random, roadside alcohol tests.

Yet, in the case of athletes, the country's offended national pride seems to be widely accepted as sufficient reason to ignore a fundamental principle of freedom. If we can justify the intrusions necessary to test athletes, and perhaps Mr. Justice Dubin will conclude that we can, will it not become easier for employers to justify intrusions into the bodies of their employees or potential employees? Canada's inquiry into drug use by athletes may have an impact on our philosophy of individual privacy which will not end in the sports arena or at the locker room door.

The principle reason why these annual reports have expressed concern about computer matching — the comparison of unrelated data bases to compile profiles of certain individuals — is because it represents search and seizure of records without reasonable cause. For the same reason, the Privacy Commissioner will continue to monitor developments in biotechnological screening programs in an effort to protect the privacy of innocent individuals.

Computer Security

"...security is concerned with protecting the computer from people; privacy with protecting people from computer"

(Robert P. Bigelow)
Computer Law and Security Report,
March/April 1989

Would it were as simple! In highly automated office environments, good computer security is essential to protecting people from other people — perhaps the ultimate goal of privacy advocates.

A totally secure computer system would appear to be an unattainable ideal in the current decentralized data processing world. Computer security professionals now talk of "trusted" rather than "secure" computer systems. (It's a telling social comment that the term "trust" now implies a measure of distrust!)

We are now in the young adulthood of the age of management information systems (MIS). Since the mid-70s the ability of the computer to perform multi-processing, to manipulate massive files, to pass information over great distances in seconds and to allow many users to share the information resource has proven an integral part of the administration of government.

It is no longer uncommon to enter a government office and find multi-purpose workstations connected to a mainframe computer system or to a network of computers wherein the data and, in some cases, the logic programs are purposefully or unwittingly shared.

Over the past year the Office of the Privacy Commissioner delved into the labyrinth of computer security — a confusing world of specialized terminology and technology. Internal threats to computer systems come in strange forms: salamis, trap doors, logic bombs, Trojan Horses, and worms. External threats are equally exotic: viruses, spoofing, scanning, switcheroo, network weaving and pass through.

And those who seek to counter these threats also "colour" the issue; in the U.S. the Department of Defence security standards are published in the "Orange Book" and explained in the "Yellow Book". The security of net-working systems are dealt with in the "Raspberry Book" — and so it goes.

The security challenges which the MIS environment poses are enormous and the Office of the Privacy Commissioner is in its infancy in developing the expertise to pinpoint problems and offer responsible, workable solutions. In the coming year, special emphasis will be placed on the security of EDP systems during our regular privacy audits of government institutions.

Special tribute should be paid to the work of the System Security Centre of the Communications Security Establishment. The Centre was established in August of 1988 to augment the computer security expertise of the RCMP and DND and to provide new capabilities for the evaluation of computer and network security products for the Government of Canada. Part of the impetus driving Canada to develop its own trusted computer security evaluation criteria was the *Privacy Act*. There was a recognition that, although the protection of national security information poses the most difficult technical problems, the most widespread problem was the need to protect the privacy of personal information held by government.

The Privacy Commissioner welcomes this initiative and looks forward to a continuing exchange of information and ideas with the Systems Security Centre.

CSIS Files

Another collection of highly-sensitive personal information continued to be a matter of concern over the past year — the intelligence files inherited by the Canadian Security Intelligence Service (CSIS) from the former Security Service of the RCMP. Much of the information contained in these files does not, at least in the view of the Security Intelligence Review Committee, meet the tests for collection under the *CSIS Act* now that the definition of “threats to the security of Canada” has been more precisely drawn.

Thus, CSIS finds itself in the awkward position of being the custodian of information about individuals which it would not be entitled to collect under the terms of its present mandate.

The solution seems simple — dispose of the old files!

In fact, CSIS has set up a unit to review the files, extract what is of continuing legitimate significance to CSIS and dispose of the rest. But, the process is laboriously slow; — some of these files have been “sequestered”, others have become subject to special rules governing internal access to and use of the files. Consultations are in progress between CSIS and the National Archives to determine what information should be archived and under what conditions.

Yet, the shredders do get used! Since the lifting of the file destruction moratorium imposed in 1985 (after concerns were expressed by the Deschênes Commission on war criminals), some 120,000 security service files have been disposed of. This includes 67,000 which had previously been scheduled for destruction by the RCMP, and 53,000 reviewed prior to disposal by CSIS. It is comforting that the review has resulted in CSIS keeping fewer than 100 files. There remain, however, many thousands of files whose appointment with the shredder is years away.

These old RCMP files create a further complication for CSIS. As authorized under the *Privacy Act*, CSIS will neither confirm nor deny the existence of information which is of continuing intelligence value. Such information is contained in bank SIS/P-PU-010. Neither will it confirm nor deny the fact that no information exists when a *Privacy Act* request is made to that bank. Both the Privacy Commissioner and the Federal Court of Canada have accepted that the so-called “mosaic effect” requires CSIS to take this approach.

However, CSIS will confirm the existence of certain personal information which was gathered by the former RCMP Security Service. Dated, less sensitive information of this type is maintained in bank SIS/P-PU-015. Its existence will be confirmed and the information will be released to a requestor subject to any of the specific exemptions which are set out in the *Privacy Act*. It has not proved possible to reach agreement with CSIS on a set of guidelines which would define what constitutes “less sensitive” information, this despite a genuinely good faith effort on the part of CSIS to respond to the concerns raised by the Privacy Commissioner in his last annual report.

As requests are received, CSIS decides where to allocate (bank 010 or 015) the former RCMP Security Service intelligence information. This appears to be the only practical approach until all records are disposed of which do not meet the *CSIS Act's* collection requirements.

The Privacy Commissioner is pleased to report that CSIS plans to accelerate its review and disposal of files. In the next two years it intends to review for disposal twice as many as during the past five years. The Privacy Commissioner applauds the initiative but considers the process should be independently monitored to ensure that all information which does not meet the "strictly necessary" requirement of section 12 of the *CSIS Act*, is actually disposed of and not merely recycled into other formats.

The Inspector General (under sections 30 and 31 of the *CSIS Act*), the Security Intelligence Review Committee (under section 40 of the *CSIS Act*) and the Privacy Commissioner (under section 37 of the *Privacy Act*) all appear to have the power and mandate to provide such independent inspection.

The Privacy Commissioner will, in the coming months, consult with the relevant parties to determine how this file disposal monitoring can be carried out without unnecessary duplication of effort.

What's with the Cheque?

Mailing lists are a private sector privacy issue which everyone understands. But few in the private or public sector have mailing lists as up-to-date and complete as the federal government.

Consider just three.

- the government's own employees (including the armed forces and the RCMP) 350,000;
- family allowance/old age pension/Canada Pension Plan recipients' list, (approximately 5.5 million names and addresses);
- and the income tax list (about 17 million).

These three lists would be a veritable gold mine for direct mailing. Some brazen requests for them have already been made.

Item: A publishing house asked Health and Welfare for the list of all Canada Pension Plan recipients and applicants. The reason? To send an advertising brochure offering legal services to anyone with a pension problem.

The federal government is prohibited from selling (or giving away) its mailing lists. But what about the government's own use of its lists. Government departments and agencies have recognized government cheque envelopes as a cost-efficient method of communicating with their clients. The cost of enclosures with regular government mailings pales beneath that of an advertising campaign and targets more successfully. It would even be an excellent way of advertising the blessings of the *Privacy Act*! ("Do you know your privacy rights?")

Family allowances and pension recipients are accustomed to finding information notices with their monthly cheques. Privacy violations or not?

No violation providing the information relates directly to the mandate of the department on whose behalf the cheque is issued. Thus, Health and Welfare Canada can appropriately inform pensioners of changes in benefits or remind parents to keep their children's inoculations up-to-date.

But there is potential for abuse. To its credit, this has not escaped the attention of the Treasury Board. As a result, the board now requires departments to obtain its permission to enclose material with a regular government mailing. The record is generally good. However, in spite of the closer monitoring, some five of the 50 mailings last year were unrelated to the original purpose of the mailing list.

Examples: Information on the Canada-U.S. Free Trade Agreement was offered in one enclosure which was sent to all nine million recipients of Family allowance, Old Age Security and Canada Pension Plan. Pension and salary cheques to past and present public servants were accompanied by appeals to purchase Canada Savings Bonds and to contribute to United Way campaigns.

Clearly, there are conflicting goods here. The government's own communication policy sensibly obliges departments and agencies to tell the public about their activities. Canada Savings Bonds are essential to the government's financing and individuals wanting to buy undoubtedly value knowing about the bonds and the procedures for automatic deductions. As well, the United Way depends heavily upon public servant's contributions, which are greatly facilitated by payroll deductions.

Yet, the principle in the *Privacy Act* is clear. Information collected for one purpose cannot be used for another purpose.

There will be some difficult applications of the law, some hard judgment calls. The Privacy Commissioner seeks not to be the Grinch who stole the Christmases which United Way agencies provide. But the Privacy Commissioner very much wants to stop government mailings being used for distributing political statements. Government junk mail is still junk mail.

What accompanies a government cheque bears some close watching.

Consultations are underway with Treasury Board to set guidelines to ensure government mass mailings conform with the *Privacy Act*.

Complaints Directorate

This year's startling 20 per cent increase in new complaints (1,050 compared to 691 in 1987/88) is difficult to explain. It may simply reflect a return to the pattern of a 10 per cent annual increase evident since the program began, making last year's drop an aberration for which this year's case-load compensated with a vengeance. This can be said: there is no reason to attribute the increase to growing resistance to either the letter or spirit of the *Privacy Act*.

The return to the larger numbers was accompanied by more complaints about the length of time departments took to respond to requests. This is disappointing. The Commissioner had hoped that the delay problem would resolve itself as departments gained experience. In fact, the office investigated 414 delay complaints, 243 of which were against the Correctional Service of Canada (CSC) — the result of a marked increase in applications.

Despite the substantial rise in new complaints, the Commissioner and his staff whittled away the 296 cases carried over from last year. Only four of these now remain.

Overall, investigators completed 1,028 cases during the year, an increase of 56 per cent over the preceding year. The directorate continues to reduce the time required to complete an investigation. The new performance standard for an investigation is three months (on average), with no complaints outstanding for longer than six months. At the end of the reporting year, 94 per cent of the complaints were less than six months old.

The acceleration can be partially explained by the addition of three staff positions to the directorate, given in anticipation of Crown corporations being made subject to the *Privacy Act*. By the end of the year these corporations were still not covered so the additional investigators allowed the office to keep pace with the large increase in complaints. With the directorate now fully staffed, the office is confident of continuing to meet the new performance standard — at least until the Crown corporations come on stream.

Statistics — “a rose by any other name”

The terminology in this report describing the disposition of complaints is a little different from previous years. The change makes consistent the terminology used by the departments in reporting their statistics to the Treasury Board and that of the Privacy Commissioner's office. Discussions with the board and all other parties resulted in the following:

Not well-founded (formerly “dismissed”)

Well-founded, resolved (formerly “justified”). This means that negotiations led to what the Commissioner considered a reasonable resolution of the problem. It does not always mean that the complainant was completely satisfied.

Well-founded. This signifies that there was some breach of the *Privacy Act* which was not resolved, either because material could not be found, had already been destroyed, or time limits had been exceeded. This term is also used when access has been denied and the Commissioner has threatened to take court action in order to have the information released.

Abandoned. This indicates that the complainant has withdrawn the complaint (often because the problem has been solved before the investigation begins), or has not responded to follow-up calls or letters.

Origin of Completed Complaints by Province and Territory	
Newfoundland	3
Prince Edward Island	35
Nova Scotia	17
New Brunswick	165
Quebec	240
National Capital Region Quebec	4
National Capital Region Ontario	53
Ontario	200
Manitoba	21
Saskatchewan	96
Alberta	57
British Columbia	134
Northwest Territories	1
Yukon	0
Outside Canada	2
TOTAL	1028

Cases

CEIC can seek UI medical claim details

An Ontario man objected to the amount of medical information the Canada Employment and Immigration Commission (CEIC) collected when he claimed unemployment insurance medical benefits.

The man was on modified duties at the time of his layoff because of an injury. He gave CEIC information from his doctor that stated the recuperation period and his claim was accepted. A week later, a specialist extended the recuperation period because the injury was not healing well. Later, the period was extended again. Each time he informed CEIC.

Following the second extension, CEIC asked for and received a completed form from the doctor. However, the commission found the information to be insufficient and asked for more detail. The doctor completed the form reluctantly because he considered the details privileged information.

During investigation it became apparent that the two doctors had supplied conflicting information. When this happens, CEIC requires, and is authorized to get, a diagnosis to settle the claim. The Commissioner concluded that CEIC officials were exercising prudent judgment as set out by the Unemployment Insurance regulations, by corroborating the information. He considered the complaint not well-founded.

Marriage data needed for passport

An Ottawa man complained that he had had to reveal his past and current marital status to the individual who guaranteed his passport application. He also worried that External Affairs collected too much information in his application.

Passport applications ask "if you are or have been married". The form explains that the details are needed for "identity, citizenship and/or custody of children." However, investigation revealed that the information is required in only three instances when:

- *the surname on the passport was assumed after marriage (either the spouse's surname or a combination of birth surname and spouse's surname);

- *when children are to be included on the passport (the details help determine legal custody);

- *a female applicant was married to a non-British subject prior to January 1, 1947. She may have ceased to be a British subject because of the marriage and, according to the laws at that time, not a Canadian citizen.

In all other cases, passport examiners may waive the marriage data requirement.

The Commissioner agreed that External Affairs needed the information but questioned whether the application form made it clear that it was limited to the three circumstances. External Affairs agreed to explain this on a new form.

The Commissioner rejected the position that requiring the guarantor to know marriage details was an invasion of privacy. A guarantor is not simply a witness to the applicant's signature, but attests, to the best of his or her knowledge, that the information is correct.

"Since a Canadian passport allows the bearer to enter Canada ... as a matter of right, I believe that disclosure of the information to the person attesting... cannot be viewed as an unreasonable requirement", the Commissioner said.

He considered the complaint not well-founded.

RCMP may release subpoenaed information

A lawyer involved in a lawsuit with an insurance company complained that the RCMP had, without consent, given the company's lawyer a copy of his client's statement to police.

The RCMP explained that it had discussed that portion of the file with the company's lawyer but had neither provided a copy nor allowed her to see one. However, all the information had been subpoenaed at an earlier criminal trial of another man. The RCMP produced the information in response to the subpoena and it was now part of court records. Thus, the RCMP discussed nothing which had not already been disclosed at the trial.

The complaint was dismissed because the *Privacy Act* allows government institutions to release personal information in response to a subpoena.

No charge to use *Privacy Act*

A senior citizen complained when charged \$25 to use the *Privacy Act*. He had seen information about using the Act in the *Seniors Guide to Federal Programs and Services*, a Health and Welfare Canada publication. He applied to National Archives for his employment file and to Canada Employment and Immigration Commission (CEIC) for his immigration file.

National Archives redirected his application to his former employer and shortly thereafter he received the information. However, CEIC charged him \$25 for his immigration documents. Because the guide had not mentioned a charge, he wrote to Health and Welfare suggesting it include such information.

An investigator found that CEIC staff had misunderstood the man's request. Seniors often need certified copies of landing documents to support pension applications, a service for which CEIC charges. Once CEIC realized the request was not for certified copies but simply to see the file under the *Privacy Act*, it refunded the \$25.

The complaint was well-founded/resolved.

Keep performance appraisals five years

A complaint that a department was keeping employees' performance appraisals too long ended up involving Revenue Canada/Customs and Excise, National Archives, the Treasury Board and the Privacy Commissioner.

The complainant told the Commissioner that Customs and Excise was retaining annual appraisals longer than the three years described in the *Personal Information Index*. The length of time that appraisals are held (the retention schedule) is established by National Archives in consultation with the Treasury Board. Customs and Excise considered the schedules as policy, not law, and not subject to complaint. Treasury Board, however, considers the schedules to be the law.

The Commissioner agreed to study the matter. The investigator confirmed that Customs and Excise was keeping the man's appraisal (and all appraisals) beyond three years. Through consultations involving the department, Treasury Board and National Archives, he discovered that Treasury Board had changed the retention period to five years but the department had not been made aware.

After discussion, Customs and Excise concluded that the intent of Treasury Board's policy was clear and agreed to comply with the five year period.

Test scores need expert interpretation

A lawyer preparing an appeal sought information about her client from two Correctional Service of Canada (CSC) banks. She complained when CSC withheld information.

Investigation revealed that much material in the Offender Health Care Record bank was supplied in confidence by a province, and thus CSC was obligated not to release it under the *Privacy Act*. The investigator suggested that the lawyer apply using the provincial privacy legislation.

CSC had also exempted raw psychological test data from a Psychology bank, maintaining that releasing medical information would not be in the inmate's best interests. CSC argued that releasing test results in raw form would make it subject to misinterpretation by laymen.

According to a CSC psychologist, the test is copyright and psychologists are not free to provide copies. He also argued that revealing test questions, individual responses and scores would render the test invalid — particularly in a closed population like a prison. Further, test results can vary daily according to the subject's health or mood. Again, a layman might misinterpret such variations and one-time scores.

The doctor suggested that the lawyer hire a registered psychologist as an expert witness to whom the doctor could release the documents.

The Commissioner found compelling the doctor's arguments against releasing this type of information in a prison environment and considered the complaint not well-founded.

Applicant gets reference comments only

Several potential and former RCMP members applied for information from their security clearance records and complained when the Force withheld the names of persons interviewed during the security clearance process and their comments.

The RCMP argued that it must take extraordinary care in screening police officers. For example, police officers have the power to arrest and carry firearms. Temperament and moral character are therefore of special importance. The RCMP argued that it must protect its sources to ensure candor.

After discussing the complaints with the investigator, the RCMP staff agreed to review the material. It concluded that the sources' comments could be released, but it withheld their names (or other identifying details) to protect the integrity of the inquiry.

The Commissioner agreed with the resolution and considered the complaints well-founded but resolved.

World War II hospital records gone

Despite a thorough effort by National Archives, a British Columbia man did not receive all the information he wanted from the Archives' Medical Records World War II bank.

He told the Commissioner that the material Archives sent excluded documents from his stay in a particular hospital in the 1940s. This included a form he had been required to sign stating that he would not apply for a military pension.

At the request of an investigator, Archives searched other banks but with no success. Archives found the records of the hospital (which no longer exists), but lacked those of the period covering the complainant's treatment.

The investigators then asked the Department of Veterans Affairs who also searched, without success, for the missing files.

The Commissioner concluded that the files cannot be found and that Archives had responded to the best of its ability. The complaint was not well-founded.

Informant's name withheld in tax case

A woman complained to the Manitoba Institute of Chartered Accountants that her former chartered accountant had acted unprofessionally. The institute began an investigation and applied to Revenue Canada, Taxation on the woman's behalf for her individual income tax return file.

Revenue Canada withheld some information because it either concerned another person or its release could "be injurious to the enforcement of the *Income Tax Act*".

The lawyer complained to the Commissioner.

The investigation confirmed that some of the information was about someone else and was thus properly exempt. The rest concerned a confidential source. The Commissioner agreed that release of the material could threaten enforcement of the *Income Tax Act*. However, he added that a strong argument could be made that the public good would be best served by releasing the information. Nevertheless, the *Privacy Act* gives the department discretion to decide and he did not believe that Revenue Canada had exercised the discretion improperly.

The complaint was not well-founded.

Grounds of Complaints and Investigation Results

Grounds	Aband.	Well-founded	Well-found. Res.	Not Well-founded	Total
Access	16	8	69	410	503
Use & Disclosure	6	8	7	29	50
Correction/Notation	0	1	6	10	17
Time Limits	4	317	14	79	414
Language	0	1	0	23	24
Index	0	0	0	0	0
Collection	2	1	2	12	17
Retention/Disposal	0	0	0	3	3
TOTAL	28	336	98	566	1028

Employer compares sick leave records

A woman asked the Commissioner's Office whether Canada Post, which employed both her and her husband, could use her attendance records to investigate her husband's attendance problems. Her file had been given to a supervisor to whom she does not report and her husband found one of her attendance cards in his own file.

The investigation had to determine whether it was proper to match the couple's attendance records to verify her husband's attendance.

Canada Post considered the use consistent with the purpose for its collection—to ensure that employees respect their leave entitlements in the collective agreement. Canada Post held that when management suspects abuse, it was “natural” to review attendance records “including those of two or more individuals where warranted”.

The Commissioner advised Canada Post that, while he understood the motivation, the practice appeared to contravene the *Privacy Act*. He invited Canada Post to respond before he made a final decision.

Canada Post replied that matching “supported the attendance and leave function” when management suspects employees are colluding to abuse leave. Canada Post maintained that the only option to matching records to confirm fraudulent leave claims would be an even more intrusive investigation.

The Commissioner was unconvinced. He had difficulty accepting that unregulated comparisons between the attendance records of spouses, other family members and golfing buddies were integral to attendance management. He concluded that accepting the position was tantamount to discrimination against employees whose relatives or friends also worked for the post office. He recommended that Canada Post stop the comparisons.

Canada Post did not agree but was prepared to discuss a resolution. After further negotiations, Canada Post adopted guidelines to control the practice. Under the new guidelines, individuals' attendance records will continue to be reviewed but will only be matched with those of others to generate depersonalized information or, if necessary, to confirm or disprove a pattern of common absenteeism already observed among employees.

The guidelines also restrict who may see and compare the information and to whom it may be disclosed.

Can't use tax files for discipline

A tax auditor, fired for falsifying her income tax returns, complained to the Privacy Commissioner that Revenue Canada, Taxation had breached both the *Income Tax Act* and the *Privacy Act* when it used her tax returns for disciplinary purposes.

A week prior to filing the complaint, the woman had asked the Federal Court to declare that Revenue Canada could not use the tax return information, except as allowed by the *Income Tax Act*. In particular, she argued that her tax returns should not be used as evidence in a hearing about her discharge.

The Commissioner postponed his finding until the court ruled. The judge agreed that when Revenue Canada is acting as an employer, it is not entitled to use individual tax returns for personnel purposes.

The *Privacy Act* allows the department to use personal information only for the purpose for which it was collected, "subject to any other act of Parliament". Since the use was not one for which it was gathered, nor was it a correct use under the *Income Tax Act* according to the court, the Commissioner concluded that the complaint was well-founded.

This does not mean that Revenue Canada may not discipline employees who evade taxes. It does mean that the department should treat the employee as it would anyone else it suspects of tax evasion, then take appropriate disciplinary action if he or she is found guilty.

Ham radio operators' data released

An amateur radio operator complained because the Department of Communications (DOC) releases amateur broadcasters personal information to amateur radio societies and publishers to print directories (call books) of licensed operators. DOC maintains a database of the licensees which includes names and addresses.

The operator opposed release of his personal data because he did not want to become the target for "junk" mail or thieves seeking expensive radio equipment.

The complaint influenced DOC to put on hold release of the information pending the Privacy Commissioner's decision. This prompted a barrage of calls and letters from operators to both DOC and the Commissioner's office.

The investigation found that DOC release of the information is a complicated issue. DOC officials told the Commissioner why the department considers the release "consistent with" the purpose for its collection.

DOC explained that it is responsible for managing the radio spectrum, a limited public resource. Individuals who pass the examinations are assigned a call signal and are licensed to use a portion of the public air waves. Publicly identifying these operators allows them to police themselves since misuse by amateurs can interfere with other radio transmission. As radio saturation and electro-magnetic interference grows, DOC considers this policing an important part of spectrum management. DOC also argued that it was not sound public policy to allow individuals to enjoy a shared resource with anonymity.

As a member of the International Telecommunication Union, DOC is obligated to provide public access to names, addresses and call signs under two articles of international regulations which deal with investigating interference, communication amongst operators and their self-training.

As well, DOC discloses licensing information to permit communication amongst amateurs, including verifying signals and technical details. This helps operators who are required by the radio regulations to confirm that a contact is a licensed amateur. DOC is also required to release the names and licence status of amateurs using shared systems (such as satellites) which are funded and maintained by the amateur community.

DOC agreed that not all operators want to join clubs, volunteer for emergency communications services or be listed in call books. However, it considered that amateurs may not opt out of their responsibility to make public their use of the airwaves.

The Commissioner accepted DOC's strong case for disclosure and noted that operators may ask private call book publishers not to list their information. He considered the complaint not well-founded.

Solicitor-client privilege widely drawn

A woman involved in a wrongful dismissal suit against Transport Canada applied for her information in its 20 standard employee banks. Her complaint alleged slow response and the withholding of material.

The investigation found that there was no information about the woman in 14 of the banks. It was also evident that information had been withheld from the grievance file, some because it concerned another person and some because the department considered that it was protected by solicitor-client privilege.

The investigator found that Transport Canada had exempted the request for its lawyer's opinion, the opinion itself, and all the background material. This material — part of the regular grievance file — was withheld in order to seek a legal opinion. The department held that once this information was attached to the request for legal advice, it became privileged.

However, legal precedents are clear that solicitor-client privilege covers communications between the parties and materials created or obtained specifically for litigation. All documents given by a client to a legal adviser are not privileged. For example, when facts are obtained from other sources, not for or by legal counsel, they are not privileged.

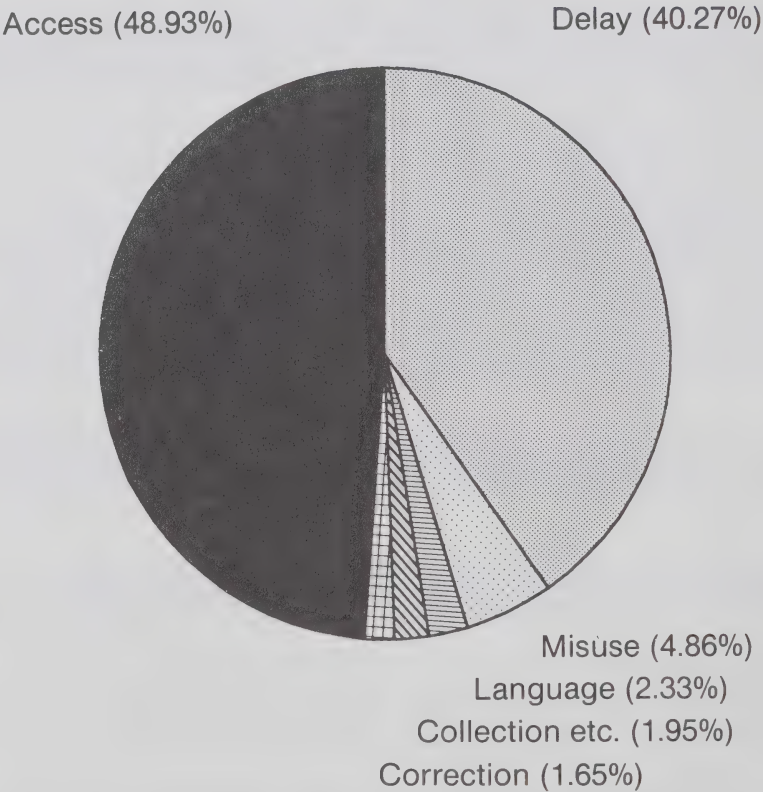
The Commissioner advised Transport Canada that he considered its view "extends unacceptably the concept of privilege". His recommendation to release the grievance file material prompted the department into partial release of the information. The Commissioner proposed to the complainant that he take her case to the Federal Court. She agreed and the Commissioner notified the department. In the meantime, Transport Canada had received advice from the Department of Justice and decided to release the material. The Commissioner considers the complaint well-founded.

Completed Complaints by Department, Type and Result

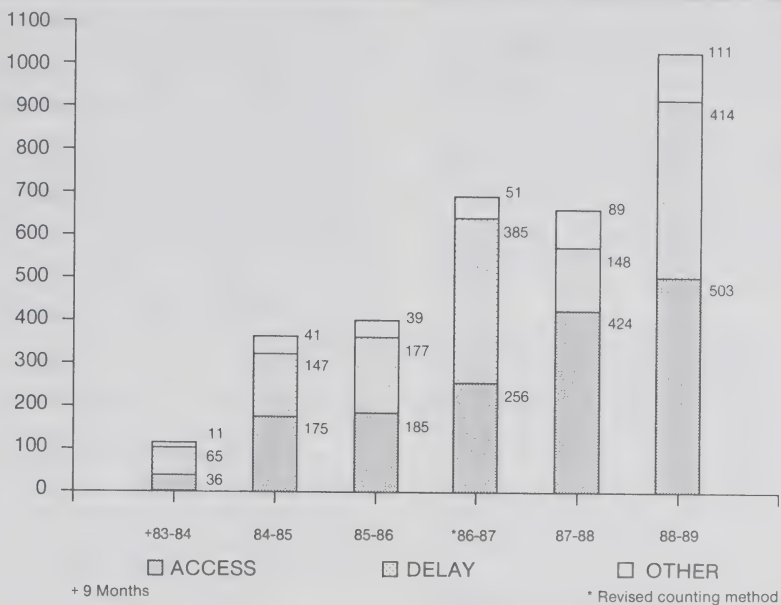
Department	Total	Well-founded	Well-founded - Resolved	Not Well-founded	Dis-continued
Agriculture Canada	5	0	2	3	0
Canada Labour Relations Board	1	0	0	1	0
Canada Mortgage and Housing Corporation	1	0	1	0	0
Canada Ports Corporation	4	0	4	0	0
Canada Post Corporation	12	2	2	7	1
Canadian Human Rights Commission	11	0	2	9	0
Canadian Security Intelligence Service	49	3	6	40	0
Communications, Department of	2	1	1	0	0
Consumer and Corporate Affairs Canada	1	0	0	1	0
Correctional Service Canada	404	203	29	168	4
Employment and Immigration Canada	68	24	13	28	3
Energy, Mines and Resources Canada	2	1	1	0	0
Environment Canada	3	0	0	0	3
External Affairs Canada	14	3	1	10	0
Health and Welfare Canada	18	3	5	8	2
Indian and Northern Affairs Canada	1	0	1	0	0
Justice Canada	5	0	0	5	0
Labour Canada	5	0	0	5	0

Department	Total	Well-founded	Well-founded - Resolved	Not Well-founded	Dis-continued
National Archives of Canada	15	1	0	14	0
National Defence	85	32	4	46	3
National Parole Board	30	3	11	15	1
Office of the Chief Electoral Officer	1	0	0	1	0
Office of the Commissioner of Official Languages	3	0	0	3	0
Office of the Correctional Investigator	1	0	1	0	0
Office of the Inspector General of the Canadian Security Intelligence Service	4	0	0	4	0
Privy Council Office	6	0	1	5	0
Public Service Commission	8	0	4	3	1
Public Works Canada	2	0	0	2	0
Revenue Canada - Customs and Excise	15	5	1	9	0
Revenue Canada - Taxation	37	11	0	21	5
Royal Canadian Mounted Police	109	13	6	86	4
Security Intelligence Review Committee	4	0	0	4	0
Solicitor General Canada	22	0	0	22	0
Transport Canada	77	31	2	43	1
Veterans' Affairs Canada	3	0	0	3	0
TOTAL	1028	336	98	566	28

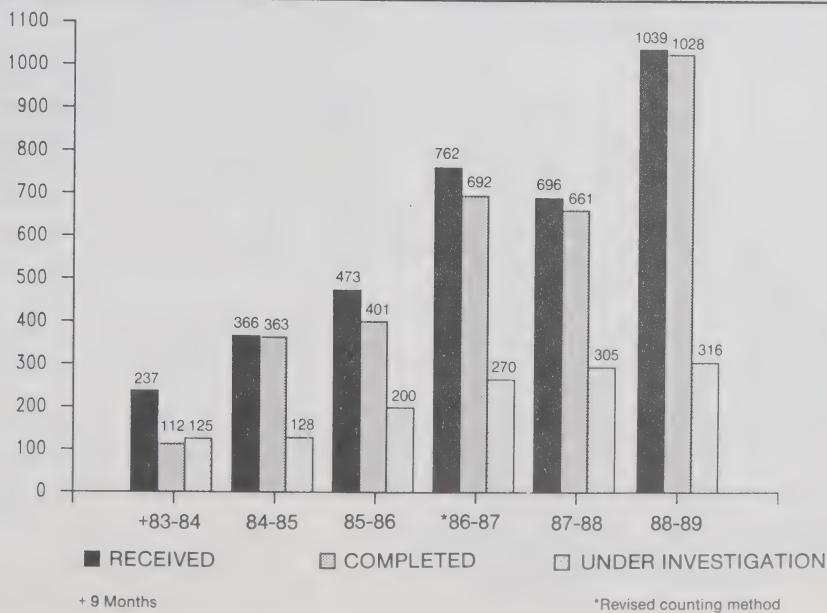
Caseload by grounds 1988-89



Completed complaints and grounds 1983-89



Completed complaints 1983-89



Inquiries

Inquiries to the Privacy Commissioner's office almost doubled in this fiscal year as the staff dealt with 2,041 compared to 1,248 in the previous year. The office now has a full-time inquiries officer who handles the majority of the calls. Her improved system of logging all inquiries makes the increase appear greater than it actually is. Before this, many calls were simply not included as staff members fielded them but lacked the time to officially record them.

Queries cover a broad range. They can be as simple as forwarding an application to see personal information to the proper department (approximately eight per cent of inquiries).

They can also be as time-consuming (but ultimately satisfying) as following up an MP's call about a detailed questionnaire which temporary helpers at Canada Post had to complete before they were hired to deliver advertising mail. Canada Post, after discussion with this office, stopped using the questionnaire. Calls about using and interpreting the *Privacy Act* make up 46 per cent of the inquiries.

Questions and complaints about the use of social insurance numbers climbed to 21 per cent of all inquiries during the year, due in large part to an amendment to the *Income Tax Act* which requires everyone to give their SIN to their financial institutions. Some callers were incensed at the apparent contradiction between the government's newly-announced policy on restricting the number and a requirement to put the SIN in the hands of their bank, trust company, credit union, caisse populaire and stockbroker. Callers were also being told they had to give it to real estate agents (who were banking deposit cheques) and to insurance agents.

Other callers were disturbed at what they considered the "secrecy" with which the new requirement was introduced. In fact, as noted earlier, the amendments to the *Income Tax Act* went through normal Parliamentary procedures. MPs did not query the new SIN requirements and the media did not report them. Most callers discovered the new law, which imposes a fine for failure to produce the SIN, when they bought the new series of Canada Savings Bonds or went to the bank. They were not amused.

About ten per cent of callers are concerned about federal agencies that are not subject to the *Privacy Act*, often Crown corporations such as Air Canada and Canadian National Railways. Some Crown corporations are expected to be covered by the Act in 1989.

Fifteen per cent of the calls concerned privacy issues in either the provincial or private sector and thus were beyond the authority of this office. For example, an Ontario woman called to determine whether the *Privacy Act* would prevent her municipality from selling its voters list to companies or individuals. The office was unable to investigate since municipalities are not covered by the *Privacy Act* and will not be subject to the Ontario legislation until 1991. (Federal enumeration lists, by comparison, may not be sold.)

Compliance Directorate

Who Was Audited

The Commissioner's office again selected audit candidates nominating targets according to overall level of risk measured as objectively as possible.

Selected were Canada Post Corporation, the Secretariat of the Ministry of the Solicitor General and Employment and Immigration Canada. In addition to these major institutions, audits were done on several smaller institutions: the Department of Finance, the Pension Appeals Board, and the Science Council of Canada.

Small agency audits are being concluded in the Law Reform Commission, International Development Research Centre, the Canadian Cultural Property Export Review Board, Export Development Corporation and Canadian Patents and Development Limited.

How and What was Audited

Audits are conducted by teams of two to four investigators who visit selected headquarters units and a number of regional offices. Investigators review a random sample of files from selected information banks and interview managers and staff who use and control the files.

The auditors examine:

- * the institution's collection, use, disclosure, retention, disposal and security of personal information;
- * the adequacy of internal policies and compliance with central agency policy and guidelines on personal information;

* the accuracy and completeness of listings in the Personal Information Index;

* staff awareness of the *Privacy Act* and its implications for handling personal information;

* individuals' access to their personal information;

* delegation of powers by the department head.

Once the audit is completed, the auditors discuss it with the managers, focussing on any areas of non-compliance. The department first receives summaries of findings, then an audit report. In line with accepted audit practice, the reports address only those areas requiring correction.

Auditing the Auditors

Six auditors cannot in a short time cover all government agencies under the *Privacy Act's* authority. Thus, the Privacy Commissioner has always urged departments' internal auditors to audit for privacy. The year provided encouraging evidence of this happening.

The Canada Employment and Immigration Commission responded. After consulting the Commissioner's office, its internal audit bureau began a review of CEIC's personal information handling. Privacy staff then examined the auditors' working papers to determine the level of reliance they could place on the audit. That review disclosed a thoroughly professional audit which the Privacy Commissioner could accept with as much confidence as if it had been done by his own auditors. (The findings are summarized elsewhere in this section.)

What Was Found

Some findings apply to all of the agencies audited. For example, few employees outside of the access to information and privacy units know about their rights under the *Privacy Act* or understand their responsibilities for the proper collection, retention, use, disclosure and disposal of personal information.

Inadequate protection of personal information is another common finding. Operational (and even some security) staff do not yet fully understand the new government security policy, particularly those sections which deal with the protection of personal information. Nevertheless, auditors found no indications that personal information had been compromised.

Auditors again found personal information holdings that had not been identified or properly described in the *Personal Information Index*. Similarly, some uses of personal information which the institution considered "consistent" with the purpose for the original collection, were not included in the Index descriptions.

The audits underscored the need for a government-wide policy covering who may see personnel files. Such policy should consider the subtleties of the *Privacy Act* and limit the amount of personnel information managers need for discharging the legitimate demands of their positions. The current organization of most personnel files precludes segregating the information according to the "need to know" principle.

Security and Privacy

Most staff treat information security as the domain of security officers or management information specialists. Both of these groups are trained to think of security in terms of classification in the "national interest", not individual privacy. They are often not prepared to deal with the designation "protected", which now applies to all information which is personal but not in the national interest.

Treasury Board, the Communications Security Establishment, the RCMP and the Privacy Commissioner's staff have taken major steps toward creating staff awareness about the protection of personal information. Until now, this information has often not been considered as security sensitive.

Continuing consultation among these organizations has produced levels of protection that match the sensitivity of the personal information. These levels will be included in the government's security policy statement. The publication and application of this new policy should help departments realize security standards for all designated information.

Incident investigations

The office investigated one lost document incident during the year and maintained a watching brief over another department's investigation of missing records. The investigation concerned the loss of tax microfiche from the Calgary district office of Revenue Canada, Taxation. Revenue Canada told the Privacy Commissioner in October 1988 that it had lost 38 sheets out of a set of microfiche. The sheets identified employers (by code number only) and their employees by surname, initials, social insurance number, earnings, pension, unemployment insurance contributions and other deductions. Each fiche (or sheet) could contain data on more than 8,000 individuals.

The investigation began at the Ottawa Head Office. Investigators followed the procedure for producing and shipping microfiche sets and were convinced that the set would have arrived intact at its destination.

Investigators followed the fiche's trail at the Calgary District Office. Once the fiche had been opened and counted, they were put in a holding tray where they were available during the day to approximately 150 staff. At night they were locked in a cabinet, but the keys were kept in an unlocked desk drawer. The first employee who needed the set in the morning could unlock the cabinet and put the fiche in the tray. It was never determined who put out the set on the day the loss was discovered. The 38 fiche were never recovered.

It became apparent that employees could remove fiche from the set and take them to other parts of the floor without completing a log. Only employees from outside that work area were required to log out fiche.

The investigators considered that Revenue Canada's security was adequate for the production and distribution of the microfiche and that staff are highly security conscious. However, once inside a secure area, employees appeared to overlook the need to protect personal information as evidenced by the cabinet key in an unlocked desk drawer. Employees also knew little or nothing about the *Privacy Act* and the obligations it imposes on employees handling personal information.

Following the incident, the office instituted new strict procedures. The set of fiche and readers are now kept and used in a secure room which is staffed while open. Sheets must be logged as used and the set then returned to a locking cabinet. Stringent controls are now in place for destruction of old fiche.

These new controls make redundant any recommendations to increase security in the Calgary unit. However, the Commissioner recommended that other locations review their storage and microfiche handling to ensure compliance with both the *Privacy Act* and the new government security policy. As well, several recommendations made after the previous microfiche theft (Annual Report 1986-87) from the Toronto office were repeated:

- * employees should be made aware of their obligations to protect personal information under the *Privacy Act*;
- * microfiche should be given even more stringent protection than paper files and
- * staff should have access to microfiche only as they need to know.

In the second incident, Correctional Service Canada lost more than 30 boxes of outdated inmate files which were being shipped to the National Archives Records Centre in British Columbia. After almost two weeks of searching, the trucking company found the boxes in its warehouse. There was no evidence that the boxes had been opened. However, standard security precautions could have prevented the incident.

The Audits

Two of this year's audits revealed a potential glitch which generated discussion between the Commissioner's office and the organizations being audited. Canada Post and the Export Development Corporation (both Crown corporations) are subject to the *Privacy Act* but technically are not bound by the federal government security policy. Both corporations have opted into the national interest provisions of the policy, but objected to the office using it as a standard against which to measure their physical security.

The Commissioner does not believe that Crown corporations should be bound necessarily by the policy but considers the government standards a reasonable measurement against which to assess the corporations' security.

Canada Post

The auditors travelled to Ottawa Head Office and divisional headquarters in Edmonton, London, and Quebec City.

Findings

Staff Awareness: As in most government institutions audited, the staff did not understand their own or others' privacy rights, nor their responsibilities under the *Privacy Act*. Canada Post publishes periodic reminders in its internal bulletins, but most staff could not recall such material. Thus, either the information is not distributed widely enough or it is simply having little impact.

Canada Post plans a communications program to support its corporate policy on the protection of personal information.

Personal Information Index Descriptions:

1.) The description of two Human Rights banks (CPC/P-PU-096 and P-PE-809) contained no reference to personal harassment cases found in the files. The bank description will be changed to incorporate a reference to the material.

2.) Change of address cards are now described as being a "class" of personal information. However, the *Privacy Act* requires that personal information used for an administrative purpose be included in an information "bank". Since the cards are used to redirect customers' mail (an administrative purpose) Canada Post will create a new bank to contain address change notices. A second bank has been established (CPC/P-PU-120) for requests from other departments to find individuals who owe Crown debts.

Protection of personal information:

Divisional headquarters employees who want to review their personnel files must apply through their supervisors and then examine the files in their presence. This means supervisors have access to all personal information in an employee's file—including such details as medical history, charitable contributions and marriages. This information is unnecessary to supervision. Canada Post will review and correct its access procedures.

Some headquarters personnel files contained limited information on other employees, usually in lists containing names and social insurance numbers. Information about third parties will be removed as the files are drawn and used.

In Edmonton, auditors found waste paper containing personal information being sent for disposal to a private company where it was stored outside and unsecured. Canada Post will ask National Archives to provide secure disposal of sensitive waste wherever possible. Elsewhere it will dispose of its own material.

The auditors also found problems with disposal of other waste materials and control of cabinets or rooms containing personal files. Canada Post is committed to correcting these problems when it implements its new privacy and security policies.

At Ottawa and Edmonton, personal information from the Risk Management Claims bank is shared with private insurance adjusters. However, no formal agreement exists with the company to ensure protection of information according to the *Privacy Act*. Canada Post will obtain insurance adjusters' undertakings to meet both

the spirit and intent of the act. It will also determine whether Canada Post should incorporate privacy and security provisions in contracts with all agents collecting or receiving personal information on its behalf.

Improper use of personal information:

Investigators found a human rights training manual which included actual grievance files, complaints and investigation reports. The documents have now been made anonymous.

Improper disclosure of personal information:

Canada Post shared on one occasion its mailing list of stamp collecting customers with the Royal Canadian Mint "and other reputable mailers". Canada Post considered this a "consistent use" of the information. The Commissioner did not see a reasonable connection between collecting stamps and collecting coins or other items. The exchange has already been stopped.

Retention and Disposal Schedules:

Auditors made several recommendations about storage or disposal of personal records that were being kept either too long, or not long enough (the act requires personal information be kept at least two years). Canada Post will take action on each of the recommendations.

Finally, auditors found fingerprints in personnel files in each division they visited. Apparently Canada Post once took fingerprints routinely from all employees. The Commissioner suggested that prints no longer needed should be returned to the individuals. Those still needed might better be stored in security clearance or reliability check files.

Pension Appeals Board

The Pension Appeals Board hears appeals against decisions of the Canada Pension Plan and the Quebec Pension Plan. All the files are held in Ottawa and all personal information is on paper. There are no EDP files.

Findings

Awareness: Board staff knew little about the *Privacy Act*. Management will provide the necessary training.

Personal Information Index Descriptions: The Index incorrectly says that the *Privacy Act* does not apply to any material the board holds about appeals under the Quebec Pension Plan. All personal information under the board's control is subject to the *Privacy Act* and the board will remove the statement from the listing.

Auditors found that the Employee Records bank (PAB/P-PE-801) is held and controlled by Health and Welfare Canada (HWC), and not the board. The description will be moved to HWC's listing and a statement included under the board's listing directing employees to Health and Welfare. The board also intends to create a bank called "Staff Matters" in which it will hold routine staff material.

Protection of Personal Information: During the audit investigators found keys left in the locks of cabinets containing completed files. The cabinets are in the main office and accessible to cleaning staff during the evening. The Board will ensure that keys are removed. Investigators also recommended new destruction procedures for sensitive waste.

Retention and Disposal: There is no retention and disposal schedule for appeals files, some of which date from 1967. The Board will seek National Archives advice on establishing a proper schedule.

Collection of Personal Information: Investigators found that the board receives all Canada Pension Plan Review Committee decisions and supporting evidence, whether or not an appeal has been filed. When there is no appeal, the board returns the evidence, but retains the decision. The Commissioner considers this to be collection of information outside the mandate of the board. The board will change its process for examining review committee files.

Science Council of Canada

The Science Council of Canada assesses Canada's scientific and technological resources, needs and potential and has a mandate to increase public awareness about science and technology.

All files are kept in the Council's office in Ottawa. No personal information is stored electronically or on microfiche.

Findings

Awareness: Science Council staff were generally aware of privacy principles — a rare finding among government institutions. In fact, the Council has conducted research into privacy-related matters.

Security of Personal Information: Auditors found staff members who handle personal information have not been checked for reliability, as required by the government security policy. The Council undertook to screen all employees who use protected information.

Cleaning staff is allowed into the personnel office unescorted after hours. No one checks to ensure that the door is locked after cleaners leave. The Council will instruct commissionaires to make such checks.

Index Bank Descriptions: Two groups of files containing personal information about contract personnel and Council members are not described in the Personal Information Index. The Council will describe these holdings in the next edition of the Index.

Department of Finance

The department implements financial and economic policies and programs. Its offices and some 800 employees are in Ottawa.

Findings

Awareness: Once again, employees interviewed demonstrated little knowledge of the *Privacy Act*, though the department developed procedures on the Act in 1983 and has since provided periodic briefings. Management is developing new procedures and guidelines which will be distributed to the administrative branch and the office of each assistant deputy minister.

Protection of Personal Information: Auditors found that both supervisors and official languages training staff who had no real need to know were

able to review complete personnel files. Moreover, some files contained limited information about other employees. One of the files examined contained a derogatory assessment of another employee.

The department is determining how it could sever sensitive information from these files without hindering supervisors and language staff from discharging their responsibilities.

Keys to cabinets were kept in unlocked drawers in nearby desks and waste personal information was found in regular garbage cans or recyclable-paper bins.

The keys will now be kept personally by the responsible staff member and "burn" bags will be provided for disposal of personal information.

Investigators suggested that the cabinet and room containing records of requests under the *Access to Information Act* and *Privacy Act* be locked when unattended. The department agreed.

Personal Information Index Descriptions: The department maintains records from reliability checks on its employees but does not list the information in the *Personal Information Index*. This effectively prevents employees from asking to see the information since they may not realize it is available.

Treasury Board has amended the description of this bank (one of the standard banks kept by all departments). The department will use Treasury Board's description.

Ministry of the Solicitor General—Secretariat

The Secretariat supports the Solicitor General whose responsibilities include the Royal Canadian Mounted Police, Canadian Security Intelligence Service, Correctional Service of Canada and the National Parole Board. Auditors visited the Secretariat's head office in Ottawa.

Findings

Protection of Personal Information:

Auditors found many of the same deficiencies identified in other agencies: detailed personnel files available to supervisors; lists of employees, some with social insurance numbers, in others' personnel files; files in locked cabinets—but keys in nearby unlocked desk drawers; personal information in regular garbage and cabinets left unlocked when offices are not staffed. As well, file covers for records in the Employee Personnel Record bank had neither a security classification nor "Protected" designation.

The Secretariat agreed to examine the problem of limiting access to personnel files. It will also remind staff about their security responsibilities. "Protected" folders are now used for new personnel files (or when requested) though the secretariat does not consider it feasible to convert all existing files.

Personnel files containing sensitive personal information should be marked appropriately because the investigation found that some information had been revealed "outside the organization that created or collected it".

Although the Secretariat has an adequate security procedure, investigators witnessed the offices left open and unstaffed.

Improper Use of Personal Information:

A human resources desk manual uses, as examples, copies of actual completed forms and memoranda. The material identifies individuals. Management agreed to remove the identifying information.

Retention and Disposal of Personal Information:

Employee personnel records and RCMP personnel and administrative records were retained beyond the approved period. The National Security Records bank (P-PU-026) had no disposal schedule. The Secretariat agreed to review personnel files annually and consult with National Archives and the Canadian Security Intelligence Service on disposal of the other files.

Personal Information Index Descriptions: Records of employee reliability checks are included in the secretariat's Security Clearances bank (P-SE-909) but are not described. Several banks have a National Archives approval number without the listing describing how long information is kept. Reliability checks will be included in the new standard bank created by Treasury Board. This bank, and disposal schedules for other banks, will be described in the next edition of the Index.

An Old Issue: In 1986 the deputy solicitor general agreed to purge personal information from the files in one of the secretariat's banks, Protection of Privacy (P-PU-035). The bank was then to be removed from the Index. During the audit, investigators found that the bank continues to be listed and only 200 of the 600 files have been purged. The Secretariat has assured the Commissioner that the task will be completed by September 1989.

Employment and Immigration Canada (EIC)

The Internal Audit

This audit was divided into two parts. The first was done by EIC's own internal audit bureau and focussed on protection of personal information about EIC clients. The Privacy Commissioner's role was to "audit the auditors". During the next two years the internal audit bureau will examine its personnel information banks and information in EDP files.

The second part, conducted by the Privacy Commissioner's office, was of EIC's Employee Assistance Program (EAP) files.

The internal audit's objective was broader in scope than those done by privacy auditors because EIC assessed the effectiveness of its internal administration and structures in dealing with both the *Privacy Act* and the *Access to Information Act*.

In an internal audit the Commissioner provides overall advice, when needed, and comments or makes recommendations on the department's compliance with the *Privacy Act's* rules concerning collecting, using, maintaining, disclosing and disposing of personal information.

Employment and Immigration, one of the largest federal government departments, provides employment counselling, training and referrals to millions of Canadians, administering the Unemployment Insurance Plan and screening and providing services to immigrants.

"The need for privacy protection is obvious. The whole of EIC, with its 800 offices, is a veritable repository of personal information. EIC runs on personal information", concluded the internal audit report. The Privacy Commissioner couldn't have put it better.

Findings

Staff Awareness: EIC auditors found privacy coordinators knowledgeable about the *Privacy Act* but other staff were not as well informed. As a result, there were inconsistencies in handling informal requests or requests from third parties such as provincial governments or advocacy groups. EIC has given priority to producing operational manuals for staff and will supplement these with training throughout the department.

Collection and Use of Information: The auditors found that a number of forms which collect personal information contain incomplete references to the *Privacy Act*. They suggested improving the privacy notice on the forms by adding descriptions of the data and listing the ways it is used, the bank in which it is kept and the organizations with which it is shared. They also recommended improving the description of the Unemployment Insurance Claim File bank in the Personal Information Index because it may not adequately describe all of the data in the files.

To ensure that its forms comply with the *Privacy Act*, EIC will ask program staff to refer forms which collect personal information to the Public Rights Administration Directorate for advice.

Data Matching: EIC shares (or matches) more information with other agencies than perhaps any other federal department. Matches include comparisons with Revenue Canada, Taxation data to ensure that individuals are reporting earnings and that those collecting unemployment insurance are not also working. The matches are carried out under the *Unemployment Insurance Act* and the *Immigration Act*.

The *Privacy Act* also allows matching by “an agreement or arrangement” between government agencies and with other governments, whether Canadian or international, in order to administer or enforce a law or carry out an investigation.

The internal auditors found that not all matches are governed by written agreements and that a portion of the agreements have been in effect too long to reflect current legislation. Without formal agreements, staff have insufficient guidance on what information can be shared and how it can be used. The auditors recommended providing summaries of agreements to operational staff, completing all pending agreements and then conducting a follow-up audit to ensure that EIC complies with the new Treasury Board data matching policy.

EIC will review all agreements and complete those still being considered. As well, it will report all current data matches to the Privacy Commissioner and ensure that they all are listed in the *Personal Information Index*. (The new Treasury Board matching policy requires all departments to advise the Privacy Commissioner’s office 60 days ahead of any new matches.)

Security: EIC auditors found that some service contracts with private companies do not contain privacy or security clauses, meaning that the companies may not always treat personal data in confidence. Auditors cited examples of companies or individuals providing services such as transportation, document shredding, office cleaning (particularly in offices with open shelving), interpretation, transcription, EDP and psychological diagnosis.

Auditors recommended revising regional contracts to include clauses to protect personal information according to the requirements of the *Privacy Act*, the security policy and EIC’s own regulations.

Disposal of personal information:

Clearly there was no consistent disposal of waste personal documents among EIC offices. Auditors found that some sorted waste for shredding or regular garbage; others simply put it out with disposable material from other building tenants. Since local office staff estimate that as much as 90 per cent of waste is personal information, auditors questioned the need to sort. The auditors also found that no single unit ensures that all microfiche are accounted for and eventually destroyed. The procedures varied from sending old fiche to regional offices, regional computer centres or to National Archives. The auditors suggested a standard procedure for eventual destruction of out-of-date fiche.

EIC's Security Task Force will address both the incorporation of security clauses in service contracts and the control and destruction of microfiche in its workplan.

Employee Assistance Files (EAP)

These files are among the most sensitive personal files kept by government, recording personal information of individuals undergoing counselling for health or behavioural problems. The files are seen only by the employee and the counsellor. Theft or unauthorized release could cause the employee irreparable harm.

As a result, auditing EAP files poses its own problems for both the department and the Privacy Commissioner. The Commissioner is torn between needing to ensure that the information is seen by as few as possible but requiring evidence that it is appropriately collected and protected. Thus, the auditor examines randomly selected anonymous files to determine whether the information meets privacy standards for collection, use, retention, disclosure and disposal.

In EIC's case there were no EAP files in the Ottawa office. EIC's policy is to maintain as little information as possible, passing necessary details on to outside counsellors. The decision not to maintain files is understandable, even commendable, as a method of ensuring client confidentiality. But the practice means there is no documentary evidence of uses of the information, nor that the client has consented to its release.

The Commissioner observed that the department has to make a trade-off between restricting the amount of sensitive personal information in files and the need for operational controls. He proposed that EIC re-examine its current procedures.

Auditors made several suggestions for improving physical security of the unit's records and disposal of waste containing personal data. The Commissioner recommended that EIC also make the improvements in the regional offices that kept files.

Notifying the Commissioner

Generally, the *Privacy Act* prohibits federal government agencies from releasing personal information to anyone other than the individual concerned. As with most rules, there are exceptions. In fact, the Act has 13 — from releases to comply with a warrant or subpoena, to helping validate aboriginal peoples' claims or grievances.

Among those exceptions are two which require the government agency to notify the Privacy Commissioner. The first covers releasing information "in the public interest" or to benefit the individual concerned. The notification gives the Commissioner an opportunity to advise the individual of the release if that is considered necessary. The second exception deals with releases for a use "consistent" with the purpose for which it was originally collected (but not described in the *Personal Information Index*).

The *Privacy Act* does not provide a means for the Commissioner or the individual to block release. The *Access to Information Act* gives third parties the right to court action to prevent the release of corporate information. The Privacy Commissioner believes that individuals too should be able to prevent the release of what they consider to be unwarranted and damaging release.

There were early suspicions that these exceptions to the general rule prohibiting the disclosure of personal information to third parties would prove to be the *Privacy Act* "Mack truck" clause. It was feared that there would be a full-scale release of personal information based on broad interpretations of "public interest" and "consistent" use. To prevent such abuse, the Commissioner itemized all uses of these releases in his annual report.

So far no abuse has been evident. While the office continues to examine each notification, beginning this year, only global statistics and select examples for illustrative purposes are reported. A detailed breakdown of the 24 notifications can be obtained from the Privacy Commissioner's office.

The MPs — again

Once again Employment and Immigration Canada (EIC) advised the Privacy Commissioner how it would handle MPs' requests for personal information about constituents during the federal election campaign.

The *Privacy Act* allows government agencies to release personal information to an MP who is trying to help solve a constituent's problem. Once Parliament is dissolved, however, MPs have only the status of ordinary citizens. This means, according to the letter of the law, that MPs may no longer (without the individual's consent) inquire on behalf of a constituent about foul-ups with a government agency since this would require them to see personal information.

It seems doctrinaire to impede MPs seeking to help constituents while in the legal limbo of an election period. On the other hand, other candidates may feel unfairly disadvantaged due to the incumbent's special access to government information. EIC — the department most affected — advised the Privacy Commissioner that during the election period it would once again release information without consent to former MPs since it “would clearly benefit” the person concerned [paragraph 8(2)(m)(ii)].

The Privacy Commissioner agreed to the solution — the same one used during the 1984 election. But he repeated his concern that delegating the discretion to disclose personal information to “any” EIC officer or employee increased the opportunity for abuse. Privacy staff reviewed 1479 such notifications during the election campaign.

The *Privacy Act* should be amended before the next election to clarify whether, during an election period, incumbent MPs should maintain their special access to government information when helping a constituent.

Breach of dog's quarantine period

Canada Post advised the Privacy Commissioner that it had given an Agriculture Canada veterinarian the address change of a woman who appeared to have breached her dog's six-month quarantine period. The dog had been in contact with a rabid animal and had not completed the required treatment.

The post office reached the woman directly but she did not cooperate. Although the *Animal Disease and Protection Act* does not authorize release of the information, Canada Post concluded the disclosure was in the public interest. The Commissioner did not question the release.

Inmates' names and addresses to Chief Electoral Officer

Following a Manitoba Court decision that inmates had the right to vote in the federal election, Correctional Service Canada advised the Commissioner that it would give the names and addresses of all federal inmates in Manitoba to the Chief Electoral Officer of Canada.

The list was to be used by returns officers to organize the voting in penitentiaries and was not to be given to anyone else. However, since the court decision was appealed, the inmates were not enumerated and the list was not sent.

Soviet government alerted to visitor with TB

External Affairs advised the Privacy Commissioner that it had notified Soviet public health authorities about a Canadian visitor with an infectious disease.

Health and Welfare Canada had warned External Affairs that a woman with pulmonary tuberculosis had refused medication and checked herself out of the hospital. She then travelled to the Soviet Union to visit relatives. After calling the Privacy Commissioner's office, External informed the Canadian embassy in Moscow which, in turn, notified the Soviets.

The notification was considered "in the public interest".

Spreading the Word

It has been said that if there were a privacy constituency in Canada — a group of knowledgeable, committed privacy activists — it would fit in the Privacy Commissioner's boardroom (a snug fit even for the Commissioner's own staff).

The job is no longer so lonely. In fact, two recent conferences on privacy (and access to information) filled large meeting rooms in Toronto and Ottawa hotels. A loose network of federal, provincial and unaligned privacy advocates is emerging, allied with committed records and EDP systems managers to spread the word.

The public may still be puzzled when told of a *Privacy Act* (and find it faintly hilarious that there is a Privacy Commissioner). Nevertheless, people understand the issues and find them deadly serious.

The Commissioner and his staff welcome opportunities to discuss the Act and the issues. During the year the Commissioner completed a series of some 20 speeches to Canadian Clubs across the country, spoke to (among others) trainee intelligence officers, data processors, heads of federal government agencies and middle level financial managers. He also participated in a Canadian Chamber of Commerce briefing on the implications for the private sector of privacy legislation and the OECD guidelines; and on AIDS at a National Parole Board seminar.

The Commissioner began a series of visits to federal penitentiaries to discuss the *Privacy Act* with staff and inmates. So far he has visited the Prison for Women in Kingston and the medium security institution at Springhill, Nova Scotia.

The Commissioner's staff continues to brief participants on the government's management training courses and spoke to Coast Guard staff in Halifax, a race relations seminar in Montreal, and college classes in Toronto and Ottawa.

The office produced an information package entitled "Do you need help using the *Privacy Act*?" It includes a poster, bookmark and an explanatory brochure describing the Commissioner's role and how to use the office's services.

Corporate Management

Corporate Management provides both the Information and Privacy Commissioners with financial, personnel, administrative, data processing and library services.

Finance

The Offices' total resources for the 1988-89 fiscal year were \$5,074,000 and 69 person-years, an increase of \$1,152,000 and 11 person-years over 1987-88. Personnel costs of \$3,837,201 and professional and special services expenditures of \$702,567 accounted for more than 88 per cent of expenditures. The remaining \$603,137 covered all other expenses.

Personnel

A substantial increase in person-years for the Privacy Commissioner produced a very active personnel program. New positions were classified and there were 42 staffing actions including two senior management appointments. In addition, the offices underwent a biennial classification audit by Treasury Board and the PM (program management) and IS (information services) positions were reviewed in line with the new classification standards.

The following are the Offices' expenditures for the period of April 1, 1988, to March 31, 1989.

	Information	Privacy	Corporate Management	Total
Salaries	\$ 1,268,673	\$1,469,048	\$568,480	\$3,306,201
Employee Benefit Plan Contributions	202,500	246,600	81,900	531,000
Transportation and Communication	29,363	66,204	118,094	213,661
Information	57,681	38,815	1,526	98,022
Professional and Special Services	506,936	144,959	50,672	702,567
Rentals	2,898	64	5,294	18,256
Purchased Repair and Maintenance	1,337	5,112	21,940	28,389
Utilities, Materials and Supplies	9,957	14,738	37,264	61,959
Acquisition of Machinery and Equipment	43,232	85,986	48,464	177,682
Other Payments	1,630	1,569	1,969	5,168
TOTAL	\$2,124,207	\$2,073,095	\$ 945,603	\$5,142,905

Administration

The offices moved to the 3rd and 4th floors of Tower B, Place de Ville. Improved security measures were implemented for the new premises and a security manual was prepared. In addition, National Archives completed a records management audit.

Informatics

A review of informatics was undertaken with the assistance of outside consultants. The office will implement the major recommendations of the study concerning renewal of the case management system and expansion of report and text production facilities.

Library

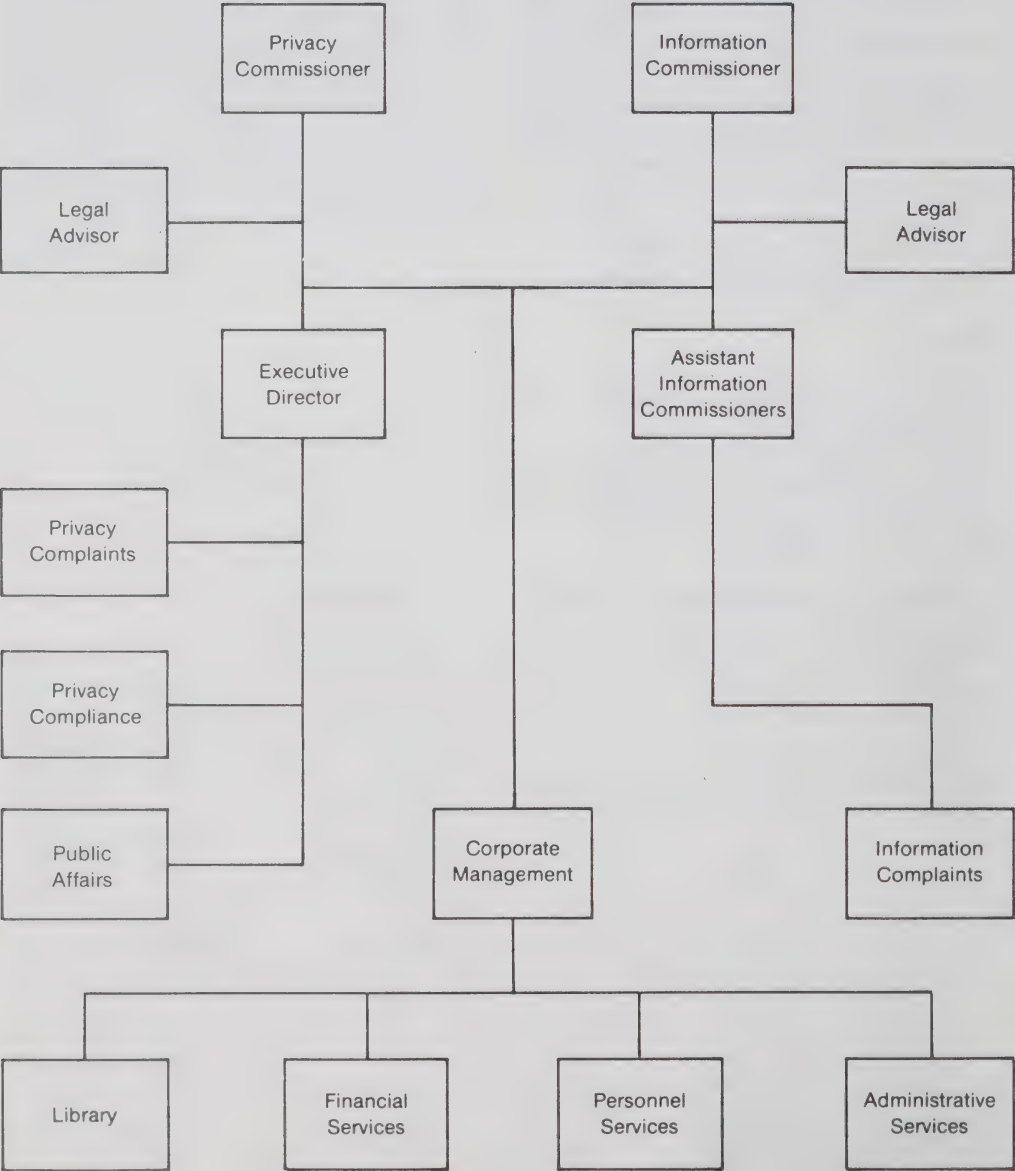
The library continues to provide an information and referral service for both Commissioners. It offers a full range of library services, including interlibrary loan, automated reference, and literature searches.

Last year, approximately 500 publications about access to information, the protection of privacy and the ombudsman function were added to the library's inventory. The public is welcome to consult our collection, which also includes newspaper clipping files, periodicals, and annual reports.

Appendix I



Offices of the
Information and Privacy
Commissioners of Canada



Appendix II

Government Institutions Covered by the Act

Advisory Council on the Status of
Women

Agricultural Products Board

Agricultural Stabilization Board

Agriculture Canada

Atlantic Development Council

Atlantic Pilotage Authority

Atomic Energy Control Board

Bank of Canada

Bilingual Districts Advisory Board

Board of Trustees of the Queen
Elizabeth II Canadian Fund to
Aid in Research on the Diseases of
Children

Bureau of Pension Advocates

Canada Council

Canada Deposit Insurance
Corporation

Canada Employment and Immigration
Commission

Canada Labour Relations Board

Canada Lands Company Limited

Canada Mortgage and Housing
Corporation

Canada-Newfoundland Offshore
Petroleum Board

Canada-Nova Scotia Offshore
Petroleum Board

Canada Ports Corporation

Canada Post Corporation

Canadian Aviation Safety Board

Canadian Centre for Occupational
Health and Safety

Canadian Commercial Corporation

Canadian Cultural Property Export
Review Board

Canadian Dairy Commission

Canadian Film Development
Corporation

Canadian Government Specifications
Board

Canadian Grain Commission

Canadian Human Rights Commission

Canadian Institute for International
Peace and Security

Canadian International Development
Agency

Canadian International Trade Tribunal

Canadian Livestock Feed Board

Canadian Patents and Development
Limited

Canadian Penitentiary Service

Canadian Pension Commission

Canadian Radio-television and
Telecommunications Commission

Canadian Saltfish Corporation

Canadian Security Intelligence Service	Freshwater Fish Marketing Corporation
Canadian Unity Information Office	Grain Transportation Agency Administrator
The Canadian Wheat Board	Great Lakes Pilotage Authority, Ltd.
Communications, Department of	Hazardous Materials Information Review Commission
Consumer and Corporate Affairs Canada	Health and Welfare Canada
Defence Construction (1951) Limited	Historic Sites and Monuments Board of Canada
The Director of Soldier Settlement	Immigration and Refugee Board
The Director, The Veterans' Land Act	Indian and Northern Affairs Canada
Economic Council of Canada	International Development Research Centre
Employment and Immigration Canada	Investment Canada
Energy, Mines and Resources Canada	Jacques Cartier and Champlain Bridges Incorporated
Energy Supplies Allocation Board	Justice Canada
Environment Canada	Labour Canada
Export Development Corporation	Laurentian Pilotage Authority
External Affairs Canada	Law Reform Commission of Canada
Farm Credit Corporation	Medical Research Council
Federal Business Development Bank	Merchant Seamen Compensation Board
Federal Mortgage Exchange Corporation	Metric Commission
Federal-Provincial Relations Office	National Archives of Canada
Finance, Department of	National Arts Centre Corporation
Fisheries and Oceans Canada	The National Battlefields Commission
Fisheries Prices Support Board	National Capital Commission
The Fisheries Research Board Canada	

National Defence	Office of the Custodian of Enemy Property
National Design Council	
National Energy Board	Office of the Director of Investigation and Research
National Farm Products Marketing Council	Office of the Inspector General of the Canadian Security Intelligence Service
National Film Board	Office of Privatization and Regulatory Affairs
National Library	
National Museums of Canada	Office of the Superintendent of Financial Institutions Canada
National Parole Board	Pacific Pilotage Authority
National Parole Service	Pension Appeals Board
National Research Council of Canada	Pension Review Board
National Transportation Agency (formerly Canadian Transport Commission)	Petroleum Compensation Board
Natural Sciences and Engineering Research Council	Petroleum Monitoring Agency
Northern Canada Power Commission	Prairie Farm Assistance Administration
Northern Pipeline Agency	Prairie Farm Rehabilitation Administration
Northwest Territories Water Board	Privy Council Office
Office of the Auditor General	Public Service Commission
Office of the Chief Electoral Officer	Public Service Staff Relations Board
Office of the Commissioner of Official Languages	Public Works Canada
Office of the Comptroller General	Public Works Land Company Ltd.
Office of the Coordinator, Status of Women	Regional Development Incentives Board
Office of the Correctional Investigator	Regional Industrial Expansion
	Revenue Canada
	Royal Canadian Mint

Royal Canadian Mounted Police

Royal Canadian Mounted Police
External Review Committee

RCMP Public Complaints
Commissioner

The St. Lawrence Seaway Authority

Science and Technology Canada

Science Council of Canada

The Seaway International Bridge
Corporation, Ltd.

Secretary of State

Security Intelligence Review
Committee

Social Science and Humanities
Research Council

Solicitor General Canada

Standards Council of Canada

Statistics Canada

Statute Revision Commission

Supply and Services Canada

Tax Review Board

Transport Canada

Treasury Board Secretariat

Veterans' Affairs Canada

War Veterans Allowance Board

Yukon Territory Water Board

Office national du film	Société canadienne des postes
Office des normes du gouvernement canadien	Société d'assurance-dépôt du Canada
Office des prix des produits de la pêche	Société de développement de l'industrie cinématographique canadienne
Office des produits agricoles	Société du crédit agricole
Office des recherches sur les pêcheries du Canada	Société immobilière du Canada limitée
Office de répartition des approvisionnement- ments d'énergie	Société pour l'expansion des exportations
Office de stabilisation des prix agricoles	Solliciteur général Canada
Pêches et Océans Canada	Statistique Canada
Les Ponts Jacques-Cartier et Champlain Incorporée	Travail Canada
Revenu Canada	Travaux publics Canada
Santé et Bien-être social Canada	Tribunal canadien du commerce extérieur
Secrétariat des relations fédérales- provinciales	
Secrétariat d'Etat	
Service canadien des pénitenciers	
Service canadien du renseignement de sécurité	
Service national des libérations conditionnelles	
Société canadienne des brevets et d'exploitation Ltée	
Société canadienne d'hypothèque et de logement	
Société canadienne des ports	

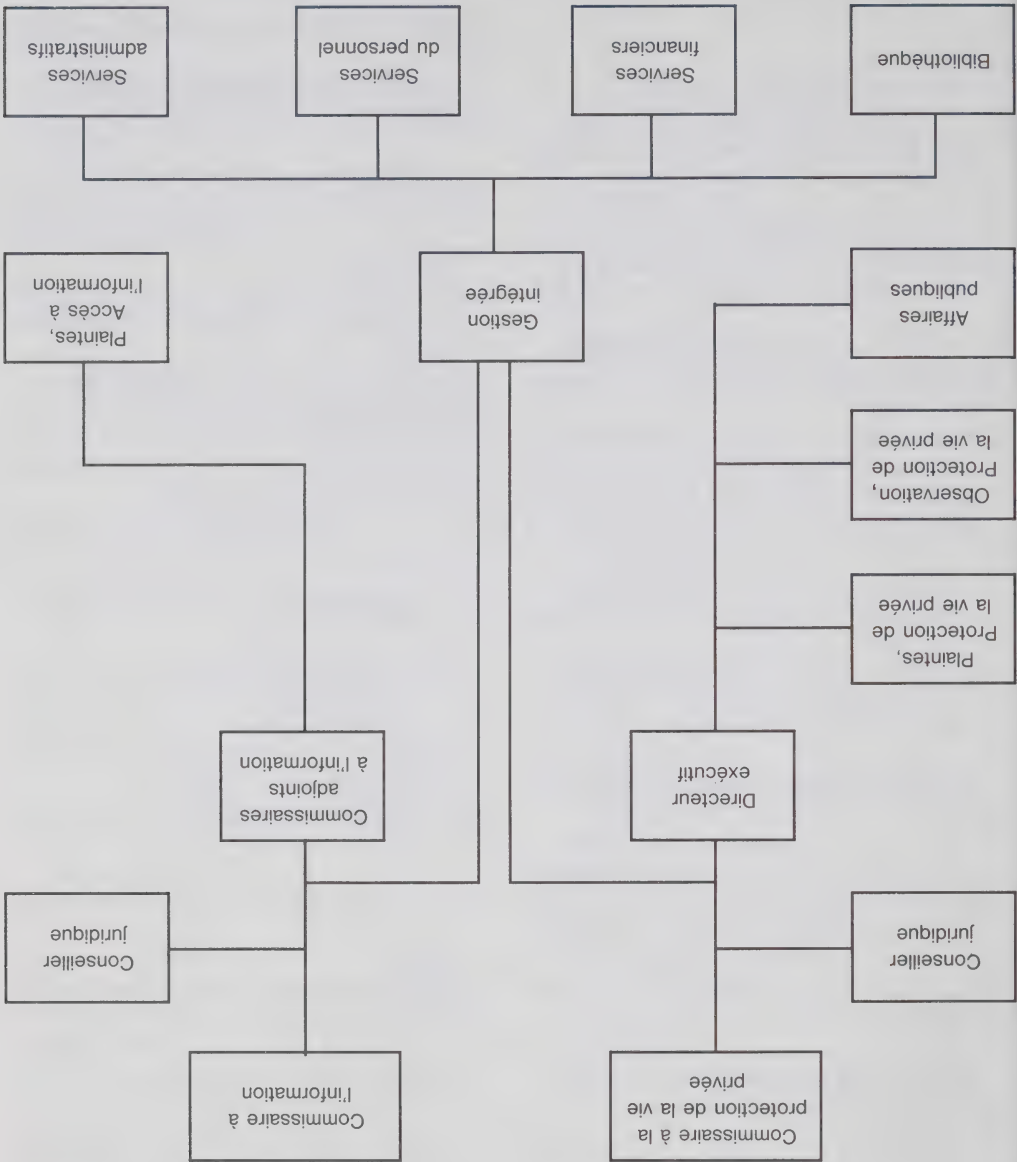
Conseil économique du Canada	Conseil de fiducie du Fonds canadien de recherches de la Reine Elisabeth II sur les maladies de l'enfance	Conseil national de commercialisation des produits de ferme	Conseil national de l'esthétique industrielle	Conseil national de recherches du Canada	Conseil de la radiodiffusion et des télécommunications canadiennes	Conseil de recherches médicales	Conseil de recherches en sciences humaines	Conseil de recherches en sciences naturelles et en génie	Conseil de révision des pensions	Conseil des Sciences du Canada	Conseil des subventions au développement régional	Conseil du Trésor, Secrétariat du	Consommation et Corporations Canada	Construction de défense (1951) Limitée	Corporation commerciale canadienne	La Corporation du Pont international de la voie maritime, Ltée	Défense nationale	Directeur de l'établissement de soldats	
Directeur des terres destinées aux anciens combattants	Emploi et Immigration Canada	Energie, Mines et Ressources Canada	Environnement Canada	Finances, Ministère des	Gendarmerie royale du Canada	Industrie, Sciences et Technologie	Institut canadien pour la paix et la sécurité internationale	Investissement Canada	Justice Canada, Ministère de la	Monnaie royale canadienne	Musées nationaux du Canada	Office Canada-Nouvelle Ecosse des hydrocarbures extracôtiers	Office Canada-Terre-Neuve des hydrocarbures extracôtiers	Office canadien du poisson saie	Office canadien des provenances	Office de commercialisation du poisson d'eau douce	Office des eaux des territoires du Nord-Ouest	Office des indemnisations pétrolières	Office national de l'énergie

Centre national des Arts, Corporation du	Comité externe d'examen de la Gendarmerie royale du Canada	Comité de surveillance des activités de renseignement de sécurité	Commissariat aux langues officielles	Commission des allocations aux anciens combattants	Commission d'appel de l'immigration	Commission d'appel des pensions	Commission canadienne des droits de la personne	Commission canadienne d'examen des exportations des biens culturels	Commission canadienne des grains	Commission canadienne du blé	Commission canadienne du lait	Commission de la Capitale nationale	Commission canadienne des pensions	Commission canadienne des transports	Commission des champs de bataille nationaux	Commission de contrôle de l'énergie atomique	Commission de l'emploi et de l'immigration du Canada	Commission d'énergie du Nord canadien
Commission de la Fonction publique	Commission de l'immigration et du statut de réfugié	Commission d'indemnisation des marins marchands	Commission des lieux et monuments historiques du Canada	Commission nationale des libérations conditionnelles	Commission des plaintes du public contre la Gendarmerie royale du Canada	Commission de réforme du droit du Canada	Commission des relations de travail dans la Fonction publique	Commission de révision de l'impôt	Commission de révision des lois	Commission du système métrique	Communications, Ministère des	Conseil des Arts du Canada	Conseil canadien des normes	Conseil canadien des relations de travail	Conseil consultatif des districts bilingues	Conseil consultatif de la situation de la femme	Conseil de contrôle des renseignements relatifs aux matières dangereuses	Conseil de développement de la région de l'Atlantique

Annexe II

Institutions fédérales assujetties à la Loi

Administrateur de l'Office du transport du grain	Administration de la voie maritime du Saint-Laurent	Administration de l'assistance à l'agriculture des Prairies	Administration de pilotage de l'Atlantique	Administration de pilotage des Grands Lacs, Limitée	Administration de pilotage des Laurentides	Administration de pilotage du Pacifique	Administration du pipe-line du Nord	Administration du rétablissement agricole des Prairies	Affaires des anciens combattants Canada	Affaires extérieures Canada	Affaires indiennes et du Nord Canada	Agence canadienne de développement international	Agence de surveillance du secteur pétrolier	Agriculture Canada	Approvisionnements et Services Canada	Archives nationales du Canada	Banque du Canada
Bibliothèque nationale	Bourse fédérale d'hypothèques	Bureau canadien de la sécurité aérienne	Bureau de l'enquêteur correctionnel	Bureau de l'inspecteur général du service canadien du renseignement de sécurité	Bureau du Conseil privé	Bureau du contrôleur général	Bureau de la coordonnatrice de la situation de la femme	Bureau du directeur des enquêtes et recherches	Bureau du Directeur général des élections	Bureau du directeur des enquêtes et recherches	Bureau du séquestre (biens ennemis)	Bureau de services juridiques des pensions	Bureau du Surintendant des institutions financières Canada	Bureau du vérificateur général	Centre canadien d'hygiène et de sécurité au travail	Centre de recherche pour le développement international	



Administration

Les Commissariats ont déménagé aux troisième et quatrième étages de la Tour B du complexe de Place de Ville. Des mesures de sécurité améliorées ont été mises en œuvre dans les nouveaux locaux et un manuel de sécurité a été rédigé. En outre, les Archives nationales ont effectué une vérification de la gestion des dossiers.

Informatique

Un examen des services informatiques a été entrepris avec l'aide de consultants de l'extérieur. Le Commissariat mettra en œuvre les principales recommandations de l'étude sur le renouvellement du système de gestion des affaires et l'expansion des systèmes de production de rapports et de textes.

Bibliothèque

La bibliothèque continue d'offrir un service d'information et de référence aux deux Commissaires. Elle dispose de toute la gamme des services de bibliothèque, y compris les prêts interbibliothèques, les systèmes de référence automatisés et la recherche documentaire.

L'an dernier, environ 500 publications sur l'accès à l'information, la protection de la vie privée et le rôle de l'ombudsman ont été ajoutées à la collection. Le public est admis à la bibliothèque pour consulter les ouvrages, les dossiers de coupures de journaux, les publications en série et les rapports annuels.

Personnel

La substantielle augmentation du nombre d'années-personnes accordées au Commissaire à la protection de la vie privée a entraîné une activité intense dans le domaine du personnel. Les nouveaux postes ont été classifiés, et il y a eu 42 mesures de dotation, dont deux nominations de cadres supérieurs. En outre, le Conseil du Trésor a pro-cédé à la vérification biannuelle de la classification de l'effectif des deux Commissariats, et les postes de PM et d'IS ont été réévalués en fonction des nouvelles normes de classification.

Finances

La Gestion intégrée fournit au Commissaire à l'information et au Commissaire à la protection de la vie privée des services dans les domaines suivants : finances, personnel, administration, informatique et bibliothèque.

Finances

Voici l'état des dépenses des Commissariats pour la période du 1^{er} avril 1988 au 31 mars 1989

Total des dépenses	2,124,207	2,073,095	945,603	5,142,905
Salaires	1,268,673	1,469,048	568,480	3,306,201
Contributions aux régimes d'avantages sociaux des employés	202,500	246,600	81,900	531,000
Transports et communications	29,363	66,204	118,094	213,661
Information	57,681	38,815	1,526	98,022
Services professionnels et spéciaux	506,936	144,959	50,672	702,567
Location	2,898	64	5,294	18,256
Achat de services				
de réparation et d'entretien	1,337	5,112	21,940	28,389
Services publics, fournitures et approvisionnements	9,957	14,738	37,264	61,959
Construction, acquisition de machines et d'équipement	43,232	85,986	48,464	177,682
Autres dépenses	1,630	1,569	1,969	5,168
Information	2,124,207	2,073,095	945,603	5,142,905
Vie privée				
Gestion intégrée				
Total				

Faites passer

On a prétendu naguère que s'il existait au Canada une confrérie de défenseurs de la vie privée, c'est-à-dire un groupe de militants avisés, elle tiendrait dans la salle de conférence du Commissaire à la protection de la vie privée. Pourtant, même le personnel du Commissaire y serait à l'étroit.

Aujourd'hui, les défenseurs de la vie privée ne sont plus aussi isolés. On l'a bien vu dans les deux conférences récentes sur la protection de la vie privée et l'accès à l'information où l'auditoire a rempli de grandes salles de réunion dans des hôtels de Toronto et d'Ottawa. Les défenseurs fédéraux et provinciaux et les promoteurs indépendants de la protection de la vie privée commencent à s'unir en un réseau non structuré qui s'allie avec des administrateurs éclairés de dossiers et de systèmes de TED pour prêcher la bonne parole.

Le public se pose peut-être encore des questions quand on lui parle de la *Loi sur la protection des renseignements personnels* (et il sourit à l'idée d'un Commissaire à la protection de la vie privée), mais il comprend la nature du problème et il en reconnaît toute la gravité.

Le Commissaire et ses collaborateurs saisissent toutes les occasions de parler de la *Loi* et des problèmes sous-jacents. Au cours de l'année, le Commissaire a prononcé une vingtaine de discours dans de nombreuses villes du pays devant divers groupes du Canadian Club, et il s'est adressé notamment à des agents de sécurité en formation, des spécialistes du traitement des données, des responsables d'organismes fédéraux et des cadres moyens spécialisés en gestion financière. Il a aussi participé à une séance d'information de la Chambre de com-

merce du Canada, au sujet des implications pour le secteur privé de la législation sur la protection des renseignements personnels et des lignes directrices de l'OCDE, et il a contribué à un séminaire sur le SIDA organisé par la Commission nationale des libérations conditionnelles.

Le Commissaire a entrepris une série de visites dans les pénitenciers fédéraux afin de parler de la *Loi sur la protection des renseignements personnels* avec le personnel et avec les détenus. Jusqu'à présent, il s'est rendu à la prison des femmes de Kingston et à Springhill, en Nouvelle-Écosse.

Le personnel du Commissariat continue à donner des séances d'information aux participants aux cours de formation en gestion du gouvernement; il s'est en outre adressé à des employés de la Garde côtière, à Halifax, ainsi qu'aux participants à un séminaire sur les relations raciales, à Montréal, et à des étudiants du niveau collégial, à Toronto et à Ottawa.

Le Commissariat a produit un ensemble d'information intitulé « Avez-vous besoin d'aide concernant la *Loi sur la protection des renseignements personnels*? » L'ensemble comporte une affiche, un signet et une brochure explicative décrivant le rôle du Commissaire et la façon de se prévaloir des services de son Commissariat.

**Le gouvernement soviétique a été
averti de la visite d'une personne
atteinte d'une maladie**

Le ministre des Affaires extérieures a
avisé le Commissaire qu'il avait averti
les services de santé de l'Union sovié-
tique de la visite en URSS d'une Cana-
dienne atteinte d'une maladie
infectieuse.

Santé et Bien-être social Canada avait
prévenu les Affaires extérieures qu'une
femme souffrant de tuberculose pulmo-
naire avait refusé les médicaments
qu'on voulait lui administrer et qu'elle
avait décidé de quitter l'hôpital. Par la
suite, elle était allée visiter des parents
en Union soviétique. Après avoir com-
munié avec le Commissariat, le minis-
tère des Affaires extérieures a transmis
les renseignements à l'ambassade du
Canada à Moscou, laquelle a averti le
gouvernement soviétique.

La divulgation a été considérée comme
d'intérêt public.

La propriétaire d'un chien n'a pas respecté la période de quarantaine.

La Société canadienne des postes a avisé le Commissaire qu'elle avait donné à un vétérinaire d'Agriculture Canada la nouvelle adresse d'une femme qui semblait n'avoir pas respecté la période de quarantaine de six mois de son chien. La bête avait été en contact avec un animal enragé, et son traitement n'était pas terminé.

La Société des postes avait communiqué directement avec l'intéressée, mais celle-ci avait refusé de collaborer. Bien que la *Loi sur les maladies et la protection des animaux* n'autorise pas la divulgation de ces renseignements, la Société a conclu que leur communication s'imposait dans l'intérêt public. Le Commissaire n'a pas contesté la divulgation.

Les noms et adresses des détenus devaient être communiqués au Directeur général des élections

Après qu'un tribunal manitobain eut décidé que les détenus avaient le droit de voter aux élections fédérales, le Service correctionnel du Canada a avisé le Commissaire qu'il communiquait au Directeur général des élections du Canada les noms et adresses de tous les détenus fédéraux incarcérés au Manitoba.

La liste des détenus devait permettre aux directeurs des élections d'organiser le scrutin dans les pénitenciers; elle ne devait être communiquée à personne d'autre. Toutefois, comme la cause a été portée en appel, les détenus n'ont pas été recensés et la liste n'a pas été envoyée.

plus s'enquérir au nom de leurs com-mettants et sans leur permission
exprime des doutes de ceux-ci avec
une institution gouvernementale, étant
donné qu'ils devraient alors consulter
des renseignements personnels.

Il semble doctrinaire de refuser d'auto-riser les députés à aider leurs commet-tants pendant une campagne électorale où leur statut est en suspens. D'un autre côté, permettre à ces députés en campagne électorale d'avoir accès à des informations gouvernementales pourrait sembler les avantager au détriment des autres candidats leur faisant la course. Emploi et Immigration Canada, l'institution gouvernementale la plus souvent sollicitée, a informé le Commissaire de son intention de conti-nuer à divulguer des renseignements personnels aux députés sortants pen-dant la campagne électorale, étant donné que « l'individu concerné en tire-rail un avantage certain », conforme-ment au sous-alinéa 8(2)m(iii).

Le Commissaire a entériné cette pra-tique, la même que pour la campagne électorale de 1984. Toutefois, il a réitéré ses réserves, en disant que la délégation de la responsabilité de divul-guer des renseignements personnels à « n'importe quel » agent ou employé d'EIC faisait augmenter les risques d'abus. Le personnel du Commissariat a donc examiné 1479 avis de ce genre pendant la campagne électorale.

La *Loi sur la protection des renseigne-ments personnels* devrait être modifiée avant les prochaines élections, pour qu'il devienne désormais légalement possible pour les députés de continuer à avoir accès aux renseignements dont ils ont besoin pour pouvoir aider leurs commettants en période de campagne électorale.

La Loi sur la protection des renseignements personnels interdit globalement aux organismes fédéraux de divulguer des renseignements personnels à quiconque sauf à l'individu concerné. Cette règle a des exceptions, comme presque toutes les règles. En fait, il y a 13 exceptions, allant des cas où les renseignements peuvent être exigés par mandat ou par subpoena, à ceux où leur divulgation peut aider les peuples autochtones à établir leurs droits ou à justifier leurs doléances.

Deux de ces exceptions obligent l'institution gouvernementale en cause à envoyer un préavis au Commissaire. La première porte sur la divulgation des renseignements « pour des raisons d'intérêt public » ou à l'avantage de l'individu concerné. La deuxième exception a trait aux divulgations « compatibles » avec les fins auxquelles les renseignements ont été recueillis, quand ces fins ne sont pas décrites dans le Répertoire de renseignements personnels.

La Loi sur la protection des renseignements personnels ne permet ni au Commissaire, ni à l'intéressé d'empêcher la divulgation. Par contre, la Loi sur l'accès à l'information donne à des tiers le droit d'en appeler aux tribunaux pour empêcher la divulgation de renseignements concernant des personnes de la vie privée estime que les particuliers devraient eux aussi pouvoir empêcher les divulgations qu'ils considèrent comme injustifiées et préjudiciables.

Au début, on craignait que ces exceptions à la règle générale interdisant la divulgation de renseignements personnels à des tiers percent une brèche monumentale dans la Loi. On redoutait une divulgation massive de renseignements personnels, fondée sur des interprétations laxistes de « l'intérêt public » et des usages « compatibles ». Pour prévenir les abus, le Commissaire a fait état de toutes les utilisations des divulgations dans son rapport annuel.

Jusqu'à présent, il ne semble pas y avoir d'abus manifestes. Même si le Commissariat continue d'étudier chaque préavis, le rapport annuel ne contiendra désormais que des statistiques globales et quelques exemples représentatifs. Cela dit, une ventilation détaillée des 24 préavis est disponible sur demande au Commissariat.

Les députés, une fois de plus

Une fois de plus, Emploi et Immigration Canada (EIC) a avisé le Commissaire de sa politique de réponse aux demandes de renseignements personnels sur leurs commentants que les députés lui adresseraient pendant la campagne électorale fédérale.

La Loi sur la protection des renseignements personnels autorise les organismes gouvernementaux à divulguer des renseignements personnels à un député qui cherche à aider un de ses commentants à résoudre un problème. Néanmoins, après la dissolution du Parlement, les députés sortants redreviennent des citoyens comme les autres. Autrement dit, si l'on s'en tient à la lettre de la Loi, ils ne pourraient

Par conséquent, la vérification des dossiers du PAE pose des difficultés particulières, à la fois pour le ministère ou l'organisme en cause et pour le Commissaire. Celui-ci est déchiré entre la nécessité de veiller à ce que les renseignements soient consultés par le moins de personnes possible et son besoin de vérifier s'ils sont recueillis et protégés convenablement. Les vérificateurs examinent donc des dossiers anonymes, choisis au hasard, afin de déterminer si les renseignements qui y sont consignés répondent aux normes de collecte, d'usage, de conservation, de divulgation et de retrait nécessaires à la protection de la vie privée.

EIC n'avait pas de dossiers du PAE dans ses bureaux d'Ottawa, en raison de sa politique de conserver le moins de renseignements possibles en communiquant les détails nécessaires à des conseillers de l'extérieur. Cette décision de ne pas conserver de dossiers est compréhensible, voire louable, car c'est un bon moyen d'assurer la confidentialité aux bénéficiaires des services. Néanmoins, il s'ensuit que la direction ne conserve pas de trace des utilisations des renseignements ni de preuve du consentement des intéressés à leur divulgation.

Le Commissaire a constaté qu'EIC avait dû accepter un compromis en tenant compte à la fois de la nécessité de limiter la quantité de renseignements personnels délicats contenus dans les dossiers et le besoin de disposer des mesures de contrôle opérationnel voulues. Il a proposé au ministre de réévaluer sa procédure actuelle.

Les vérificateurs ont fait plusieurs propositions en vue d'améliorations de la sécurité matérielle des dossiers du service et de la destruction des renseignements personnels. Le Commissaire a recommandé qu'EIC prenne les mêmes mesures d'amélioration dans ses bureaux régionaux qui conservent des dossiers.

EIC examinera tous les accords et conclura ceux qui ne l'ont pas encore été, en plus de signaler tous ses couplages de données actuels au Commissaire et de veiller à ce qu'ils soient tous mentionnés dans le *Répertoire de renseignements personnels*. (La nouvelle politique du Conseil du Trésor sur le couplage oblige tous les ministères et organismes à prévenir le Commissariat 60 jours avant tout nouveau couplage.)

Sécurité : Les vérificateurs d'EIC ont constaté que certains marchés de service avec des entreprises privées ne contenaient pas de dispositions sur la sécurité ou sur la protection des renseignements personnels, de sorte que ces entreprises risquaient de ne pas toujours traiter les renseignements de ce genre de façon confidentielle. Les vérificateurs ont donné des exemples d'entreprises ou de particuliers offrant des services de transport, de destruction de documents, de nettoyage de bureaux (particulièrement dans les bureaux à étages ouvertes), d'interprétation, de transcription, de traitement électronique des données et de diagnostic psychologique.

Enfin, les vérificateurs ont recommandé que les marchés régionaux soient révisés par l'ajout de dispositions de protection des renseignements personnels conformément aux exigences de la *Loi sur la protection des renseignements personnels*, de la politique sur la sécurité et du règlement pertinent d'EIC.

Retrait des renseignements personnels : La vérification a révélé un manque d'uniformité des méthodes de destruction des documents personnels dans les bureaux d'EIC. Dans certains cas, on trie les documents avant de les détruire en les envoyant à la déchiqueteuse ou en les mettant à la poubelle;

ailleurs, on jette simplement les documents en même temps que les déchets des autres locataires de l'immeuble. Etant donné que le personnel des bureaux locaux estime que les documents contenant des renseignements personnels constituent jusqu'à 90 p. 100 des déchets, les vérificateurs se demandent s'il vaut la peine de les trier. En outre, ils ont constaté qu'aucun service ne tient de registre de contrôle et de destruction de ses microfiches. À cet égard, la procédure varie : on peut envoyer les vieilles fiches aux bureaux régionaux, à des centres régionaux d'informatique ou aux Archives nationales. Les vérificateurs ont proposé l'adoption d'une procédure normalisée de destruction des vieilles fiches.

Dans son plan de travail, le Groupe d'EIC sur la sécurité s'intéressera à la fois à l'ajout de dispositions sur la sécurité dans les marchés de services et au contrôle et à la destruction des microfiches dans son plan de travail.

Dossiers d'aide aux employés (PAE)

Ces dossiers sont parmi les plus délicats des dossiers personnels contenus par le gouvernement; ils contiennent des renseignements personnels sur des personnes recevant des services de counselling pour surmonter leurs problèmes de santé ou de comportement. Seuls l'employé intéressé et le conseiller peuvent consulter ces dossiers. S'ils étaient volés ou si leur contenu était divulgué sans autorisation, l'employé pourrait subir un préjudice irréparable.

les demandes officielles ou celles de tierces parties, comme les gouvernements provinciaux ou les groupes de pression, n'étaient pas toujours traitées de façon uniforme. EIC s'est donné pour priorité de produire des manuels d'exploitation à l'intention de l'ensemble de son personnel, qui bénéficiera aussi de cours de formation.

Collecte et usage des renseignements personnels

La Loi sur la protection des renseignements personnels : Les vérificateurs ont constaté que plusieurs formulaires servant à recueillir des renseignements personnels faisaient état de façon incomplète de la *Loi sur la protection des renseignements personnels*. Ils ont proposé à EIC d'améliorer son texte sur la protection de la vie privée en ajoutant des descriptions des données requises, de la façon de les utiliser, du fichier où elles sont conservées et des organisations avec lesquelles elles sont partagées. Ils ont aussi recommandé une amélioration de la description du fichier des dossiers de réclamation dans l'assurance-chômage qui figurent dans le *Répertoire de renseignements personnels*, parce que la description actuelle ne reflète peut-être pas très bien toutes les données conservées dans le fichier.

Pour s'assurer que ses formules respectent la *Loi sur la protection des renseignements personnels*, EIC demandera au personnel de ses programmes de consulter la Direction de l'application des droits du public au sujet des formules servant à recueillir des renseignements personnels.

Couplage des données : EIC partage ou couple sans doute plus de données avec d'autres organismes que n'importe quelle autre composante de l'Administration fédérale. Les couplages comprennent des comparaisons de données avec Revenu Canada (impôt) pour vérifier si les particuliers déclarent leurs revenus et si les prestataires du régime d'assurance-chômage travaillent. Le couplage est effectué en vertu de la *Loi sur l'assurance-chômage* et de la *Loi sur l'immigration*.

La *Loi sur la protection des renseignements personnels* autorise aussi le couplage « aux termes d'accords ou d'ententes » entre des organismes gouvernementaux, d'autres gouvernements (soit provinciaux, soit d'autres pays) et des organismes internationaux, pour l'administration ou l'application d'une loi ou la tenue d'une enquête.

Les vérificateurs internes ont constaté que le couplage n'était pas toujours régi par des accords écrits et qu'une partie de ces accords datent de si longtemps qu'ils ne reflètent plus la législation actuelle. S'ils n'ont pas d'accords officiels pour se guider, les employés ne savent pas très bien quels renseignements peuvent être partagés et comment ils peuvent être utilisés. Les vérificateurs ont recommandé qu'on distribue des résumés des accords au personnel, que tous les accords en négociation soient conclus et qu'on procède ensuite à une vérification de suivi afin de s'assurer qu'EIC respecte bien la nouvelle politique du Conseil du Trésor sur le couplage des données.

Connaissance de la Loi sur la protection des renseignements personnels: Les vérificateurs d'EIC ont constaté que les coordonnateurs de la protection de la vie privée connaissaient la Loi, mais que les autres employés n'étaient pas aussi bien informés. Par conséquent,

Constatations

Les vérificateurs internes ont conclu que le besoin de protection de la vie privée était manifeste, étant donné qu'EIC, avec ses 800 bureaux, est une véritable mine de renseignements personnels. Sans renseignements personnels, EIC ne pourrait pas fonctionner. Le Commissaire n'aurait pas dit mieux.

Les vérificateurs internes ont conclu que le besoin de protection de la vie privée était manifeste, étant donné qu'EIC, avec ses 800 bureaux, est une véritable mine de renseignements personnels. Sans renseignements personnels, EIC ne pourrait pas fonctionner. Le Commissaire n'aurait pas dit mieux.

Le Régime d'assurance-chômage. En outre, il filtre les immigrants et leur fournit des services.

Les vérificateurs internes ont conclu que le besoin de protection de la vie privée était manifeste, étant donné qu'EIC, avec ses 800 bureaux, est une véritable mine de renseignements personnels. Sans renseignements personnels, EIC ne pourrait pas fonctionner. Le Commissaire n'aurait pas dit mieux.

Le groupe de vérification interne s'était donné des objectifs plus vastes que ceux des vérificateurs du Commissariat, étant donné qu'EIC voulait évaluer l'efficacité de son administration et de ses structures internes d'application de la Loi sur la protection des renseignements personnels et de la Loi sur l'accès à l'information.

Le second volet, réalisé par le Commissariat, a porté sur les dossiers du Programme d'aide aux employés (PAE) d'EIC.

La vérification a comporté deux volets : le premier, qui a été réalisé par le Bureau de la vérification interne d'EIC, a été axé sur la protection des renseignements personnels concernant les clients d'EIC. Le Commissariat a évalué le travail des vérificateurs internes. Au cours des deux prochaines années, le Bureau de la vérification interne d'EIC examinera les fichiers de renseignements personnels et les renseignements contenus dans les fichiers informatiques.

La vérification interne

Emploi et Immigration Canada (EIC)

Une vieille histoire : En 1986, le Soliciteur général adjoint a accepté d'éliminer les renseignements personnels contenus dans les dossiers de l'un des fichiers du Secréariat, celui de la Protection de la vie privée (P-PU-035). Ce fichier devait par la suite être retiré du *Repertoire*. La vérification a révélé que le fichier est toujours inscrit au *Repertoire* et que 200 seulement des 600 dossiers qu'il contient ont été épurés. Le Secréariat a promis au Commissaire que le nécessaire sera fait d'ici septembre 1989.

conservation des renseignements ne soit précisée. À l'avenir, les vérifications de fiabilité seront conservées dans le nouveau fichier ordinaire établi par le Conseil du Trésor. Ce fichier sera décrit dans la prochaine édition du *Repertoire*, et les normes de destruction des autres fichiers le seront aussi.

Secrétariat du Solliciteur général

Le Secrétariat est un service du Solliciteur général qui est responsable de la Gendarmerie royale du Canada, du Service canadien du renseignement de sécurité, du Service correctionnel du Canada et de la Commission nationale des libérations conditionnelles. Les vérificateurs ont visité l'administration centrale du Secrétariat, à Ottawa.

Constataions

Protection des renseignements personnels : Les vérificateurs ont constaté beaucoup de lacunes du genre de celles qui ont été relevées dans les autres ministères et organismes : les superviseurs ont accès à des dossiers personnels détaillés; il y a des listes d'emplois, certaines avec le numéro d'assurance sociale des intéressés, dans les dossiers personnels d'autres employés; les dossiers sont conservés dans des classeurs verrouillés, mais les clés sont laissées dans des tiroirs de bureau ouverts; des documents contenant des renseignements personnels sont jetés à la poubelle et des classeurs ne sont pas verrouillés quand les responsables sont absents. En outre, les couvertures des dossiers conservés dans le fichier des dossiers personnels des employés ne portent pas de mention de sécurité ou de désignation « Protégé ».

Le Secrétariat a consenti à étudier la question de la limitation de l'accès aux dossiers personnels. Il rappellera aussi à ses employés leurs responsabilités en matière de sécurité. Enfin, il utilise désormais des chemises « Protégé » pour les nouveaux dossiers personnels (ou pour les anciens, sur demande), même s'il estime qu'il ne serait pas faisable d'utiliser ce genre de chemise pour tous les dossiers existants.

Les dossiers personnels contenant des renseignements personnels de nature délicate devraient être convenablement identifiés, parce que la vérification a révélé que certains renseignements avaient été divulgués à l'extérieur de l'organisation qui les avait produits ou reçueils. Enfin, bien que le Secrétariat ait une procédure de sécurité satisfaisante, les enquêteurs ont constaté que certains employés quittaient leur bureau sans le verrouiller.

Divuligation indu : Un manuel des ressources humaines contient des exemples qui sont des copies de documents réels (formules remplies et notes de service). Des personnes sont nommées dans ces documents. La direction a accepté d'éliminer les détails pertinents.

Conservation et retrait : Les dossiers personnels des employés et les dossiers personnels et administratifs de la GRC sont conservés au-delà de la période approuvée. Le fichier des dossiers sur la sécurité nationale (P-PU-026) ne fait l'objet d'aucune norme de destruction. Le Secrétariat a consenti à passer les dossiers personnels en revue chaque année, et il a consulté les Archives nationales et le Service canadien du renseignement de sécurité au sujet du retrait des autres dossiers.

Contenu du Répertoire de renseignements personnels : Les dossiers des vérifications de fiabilité des employés sont conservés dans le fichier des Autorisations sécuritaires (P-SE-909) du Secrétariat, sans être décrits dans le Répertoire. Plusieurs fichiers ont un numéro d'approbation des Archives nationales, mais sans que la période de

Ministère des Finances

Le Ministère est responsable de la mise en œuvre de politiques et de programmes financiers et économiques. Ses 800 employés sont tous dans ses bureaux d'Ottawa.

Constatations

Connaissance de la Loi sur la protection des renseignements personnels :

Aux Finances comme ailleurs, les

employés interrogés ignoraient à peu

près tout de la Loi, même si le Minis-

tere s'est donné des procédures à cet

égard dès 1983 et qu'il les a complé-

tées depuis par des séances d'infor-

mation régulière. Les responsables

préparent de nouvelles procédures et

des lignes directrices qui seront distri-

buees à la Direction de l'administration

et au cabinet de chaque sous-ministre

adjoint.

Protection des renseignements per-

sonnels : Les vérificateurs ont constaté

que les superviseurs et les employés

chargés de la formation en langues offi-

cielles pouvaient consulter les dossiers

du personnel sans aucune restriction,

même si ni les uns ni les autres

n'avaient vraiment besoin de connaître

leur contenu. En outre, certains dos-

siers contenaient des renseignements

sur d'autres employés. Dans l'un deux,

on a même trouvé une évaluation déro-

gatoire d'un autre employé.

Le Ministère cherche des moyens de

cloisonner ces dossiers pour en retirer

les renseignements à caractère délicat

sans entraver les superviseurs et les

employés des services linguistiques

dans l'exercice de leurs fonctions.

Par ailleurs, les vérificateurs ont trouvé des clés de classeurs dans des tiroirs de bureau non verrouillés et des renseignements personnels sur du papier de rebut dans des poubelles et des contenants de papier recyclable.

Les employés responsables conservent désormais les clés sur eux et les documents contenant des renseignements personnels devront être jetés dans des sacs de déchets à brûler.

Le Ministère a accepté la proposition des enquêteurs de verrouiller les classeurs et les pièces contenant des dossiers de demandes en vertu de la Loi sur l'accès à l'information et de la Loi sur la protection des renseignements personnels quand les employés s'absenteront ou qu'ils quitteront le travail.

Contenu du Répertoire de renseignements personnels : Le Ministère conserve des dossiers sur les résultats des vérifications de la fiabilité de ses employés, mais il n'en fait pas état dans le *Répertoire*. Par conséquent, les employés ne peuvent demander qu'on leur donne accès à ces renseignements, étant donné qu'ils n'en connaissent pas toujours l'existence.

Le Conseil du Trésor a modifié la description de ce fichier (l'un des fichiers ordinaires que conservent tous les ministères). Les Finances adopteront la description du Conseil du Trésor.

Protection des renseignements personnels

sonnels : Pendant la vérification, les enquêteurs ont trouvé des clés dans les serrures de classeurs contenant des dossiers complets. Ces classeurs sont dans le bureau central, et les préposés au nettoyage y ont accès pendant la soirée. La Commission veillera à ce que le personnel ne laisse plus traîner les clés. Les enquêteurs ont aussi recommandé de nouvelles procédures de destruction des déchets posant des problèmes de sécurité.

Conservation et retrait : Il n'y a pas de période de conservation avant destruction prévue pour les dossiers d'appel, dont certains datent de 1967. La Commission demandera aux Archives nationales de lui recommander une période de conservation appropriée.

Collecte de renseignements personnels : Les enquêteurs ont constaté que la Commission reçoit toutes les décisions du Comité de révision du Régime de pensions du Canada, avec les pièces, qu'un appel ait été interjeté ou pas. S'il n'y a pas d'appel, la Commission renvoie les pièces, mais conserve la décision. Le Commissaire s'est dit d'avis que cela constitue une collecte de renseignements débordant le mandat de la Commission. Celle-ci modifiera sa procédure d'examen des dossiers du Comité de révision.

Conseil des sciences du Canada

Le Conseil des sciences du Canada évalue les ressources, le potentiel et les besoins scientifiques et technologiques du Canada; il a pour mission de sensibiliser le public aux sciences et à la technologie.

Constatations

Tous les dossiers du Conseil sont dans ses bureaux d'Ottawa. Les renseignements personnels ne sont pas conservés dans des fichiers informatiques ou sur microfilm.

Connaissance de la Loi sur la protection des renseignements personnels : Le personnel du Conseil a une connaissance générale des principes de la protection de la vie privée, ce qui est rare pour une institution gouvernementale. (Le Conseil a fait des recherches sur des questions liées à la protection de la vie privée.)

Protection des renseignements personnels : Les enquêteurs ont constaté que certains employés qui utilisaient des renseignements personnels n'avaient pas fait l'objet de l'enquête de fiabilité requise par la politique du gouvernement sur la sécurité. Le Conseil a commencé à faire enquête sur tous les employés utilisant des renseignements protégés.

Les préposés au nettoyage peuvent circuler sans surveillance dans le bureau du personnel après les heures de travail. Personne ne vérifie si la porte du bureau est verrouillée après leur départ. Le Conseil précisera aux commissions-naires comment faire les vérifications qui s'imposent.

Contenu du Répertoire de renseignements personnels : Deux groupes de dossiers contenant des renseignements personnels sur des employés contractuels et sur les membres du Conseil ne sont pas décrits dans le Répertoire. Le Conseil les décrira dans la prochaine édition.

Commission d'appel des pensions

La Commission d'appel des pensions entend des appels interjetés des décisions du Régime de pensions du Canada et du Régime des rentes du Québec. Tous les dossiers sont conservés à Ottawa et tous les renseignements personnels sont sur support papier. Il n'y a pas de fichier informatique.

Constataions

Connaissance de la Loi sur la protection des renseignements personnels : Le personnel ignore à peu près tout de la Loi. La direction lui donnera la formation nécessaire.

Contenu du Répertoire de renseignements personnels : D'après le Répertoire, la Loi sur la protection des renseignements personnels ne s'applique pas aux documents que la Commission détient au sujets d'appels portant sur le Régime des rentes du Québec. C'est faux : tous les renseignements personnels que la Commission détient sont assujettis à la Loi sur la protection des renseignements personnels. La Commission modifiera le texte en conséquence.

Les enquêteurs ont constaté que le fichier des Dossiers individuels sur le personnel (CAP/P-PE-801) relève de Santé et Bien-être social Canada plutôt que de la Commission. La description du fichier sera transférée sous Santé et Bien-être social Canada; on ajoutera à la rubrique de la Commission une déclaration renvoyant les employés au Ministère. La Commission compte aussi créer un fichier intitulé « Personnel » dans lequel elle conservera les renseignements généraux sur le personnel.

Divulgation indu : La Société des postes a partagé sa liste de distribution de philatélistes avec la Monnaie Royale canadienne et avec d'autres expéditeurs ayant une bonne réputation. La Société était d'avis qu'il s'agissait là d'un « usage compatible » des renseignements en question. Le Commissaire n'a pour sa part pas établi de rapport logique entre le fait d'être philatéliste et celui de collectionner des pièces de monnaie ou d'autres articles. Le partage de la liste avait déjà cessé. (Il s'agit d'un cas isolé.)

Conservation et retrait : les enquêteurs ont fait plusieurs recommandations sur l'entreposage ou le retrait de dossiers personnels qui avaient été conservés trop longtemps ou trop peu de temps. (En vertu de la Loi, ils doivent être conservés au moins deux ans.) La Société des postes prendra des mesures en réponse à chacune des recommandations.

Enfin, les enquêteurs ont trouvé des empreintes digitales dans des dossiers personnels de chacune des divisions qu'ils ont visitées. Il semble que la Société prenait les empreintes digitales de tous ses employés. Le Commissaire s'est dit d'avis que les empreintes dont elle n'a plus besoin devraient être rendues aux intéressées. Celles dont la Société a encore besoin devraient être conservées dans des dossiers d'autorisation sécuritaires et de vérification de la fiabilité.

de changement d'adresse. Un autre fichier a été constitué pour répondre aux autres ministères cherchant à localiser les particuliers qui sont débiteurs de l'État.

Protection des renseignements personnels :

Les employés des bureaux divisionnaires centraux qui veulent consulter leur dossier personnel doivent le demander par l'intermédiaire de leur superviseur, puis consulter le dossier en sa présence. Les superviseurs ont donc accès à tous les renseignements personnels figurant aux dossiers des employés, y compris des détails tels que leurs antécédents médicaux, leurs dons à des œuvres de charité et leur état civil. Il n'est pas nécessaire d'avoir accès à des renseignements de ce genre pour superviser. La Société des postes réévaluera ses procédures d'accès aux renseignements personnels et les corrigera.

A Edmonton, les vérificateurs ont trouvé des renseignements personnels sur du papier de rebut dont on se débarrassait en l'envoyant à une entreprise privée qui le gardait à l'extérieur, sans protection. La Société des postes demandera aux Archives nationales de lui donner des moyens de se défaire en toute sécurité des déchets à caractère

Les enquêteurs ont aussi constaté des difficultés liées à l'élimination d'autres déchets et à la protection des dossiers ou des pièces contenant des dossiers personnels. La Société des postes est déterminée à corriger ces lacunes lorsqu'elle mettra en œuvre ses nouvelles politiques sur la protection des renseignements personnels et sur la sécurité. A Ottawa et à Edmonton, le fichier de réclamations pour la gestion des risques est partagé avec des ajusteurs d'assurances du secteur privé. Toutefois, aucune entente officielle n'a été conclue avec la compagnie d'assurance pour protéger ces renseignements conformément à la Loi sur la protection des renseignements personnels. La Société des postes obtiendra des ajusteurs d'assurances l'engagement de respecter l'esprit et la lettre de la Loi. Elle devra aussi décider s'il serait préférable qu'elle ajoute des dispositions sur la protection des renseignements personnels et sur la sécurité à ses contrats avec tous les agents qui recueillent ou qui reçoivent des renseignements personnels en son nom.

Usage indu des renseignements personnels :

Les enquêteurs ont trouvé un manuel de formation sur les droits de la personne qui contenait des rapports de griefs, des plaintes et des ports d'enquêtes réels. Ces documents ont été modifiés de façon à préserver l'anonymat des intéressés.

Connaissance de la Loi sur la protection des renseignements personnels : Comme c'est le cas dans la plupart des organismes gouvernementaux qui ont fait l'objet d'une vérification, le personnel ne comprenait pas ses droits ou ceux d'autrui — pas plus que ses responsabilités — en fonction de la Loi sur la protection des renseignements personnels. La Société publie régulièrement des rappels dans ses bulletins internes, mais la plupart des employés ne s'en souvenaient pas. Autrement dit, la diffusion de ces messages est insuffisante, ou leur effet est médiocre.

La Société compte mettre sur pied un programme de communication à l'appui de sa politique générale sur la protection des renseignements personnels.

Contenu du Répertoire de renseignements personnels :

1. La description de deux fichiers sur les droits de la personne (SPC/P-PU-096 et P-PE-809) ne faisaient pas état des cas de harcèlement personnel contenus dans les dossiers. La description du fichier a été modifiée en conséquence.

2. Les cartes de changement d'adresse sont désormais décrites comme une « catégorie » de renseignements personnels. Toutefois, la Loi sur la protection des renseignements personnels dispose que les renseignements personnels utilisés à des fins administratives doivent être inclus dans un « fichier ». Étant donné que les cartes sont utilisées pour réadresser le courrier des clients (à des fins administratives), la Société des postes créera un nouveau fichier qui contiendra les avis

Deux des vérifications réalisées cette année ont révélé une anomalie qui pourrait causer des problèmes, et qui a entraîné des discussions entre le Commissariat et les organismes en cause, la Société canadienne des postes et la Société pour l'expansion des exportations, deux sociétés d'État qui sont assujetties à la Loi sur la protection des renseignements personnels et qui, en théorie, ne sont pas liées par la politique du gouvernement du Canada sur la sécurité. L'une et l'autre ont choisi de respecter les dispositions de la politique en matière d'intérêt national, mais elle se sont opposées à ce que le Commissariat s'en serve comme normes d'évaluation de leurs mesures de sécurité matérielle.

Le Commissaire ne croit pas que les sociétés d'État devraient nécessairement être liées par la politique du gouvernement, mais il estime que les normes gouvernementales sont un critère raisonnable d'évaluation de leurs mesures de sécurité.

Société canadienne des postes

Les vérificateurs ont visité l'administration centrale de la Société, à Ottawa, ainsi que les bureaux divisionnaires centraux d'Edmonton, de London et de Québec.

Les enquêteurs se sont rendu compte que les employés pouvaient sortir des fiches du jeu et les emporter dans d'autres locaux de l'étage sans signer de registre. Seuls les employés ne travaillant pas dans le service en question étaient tenus de signer un registre pour en sortir des fiches.

Tout compte fait, les enquêteurs ont jugé que les mesures de sécurité de Revenu Canada étaient suffisantes pour la production et la distribution des microfiches et que les employés étaient très sensibilisés aux questions de sécurité. Toutefois, une fois rendus dans un bureau « sûr », ils semblaient négliger la nécessité de protéger les renseignements personnels; le fait que la clé de l'armoire était dans un tiroir non verrouillé le montre bien. En outre, les employés ignoraient à peu près tout de la Loi sur la protection des renseignements personnels et des obligations qu'elle impose au personnel utilisant des renseignements de ce genre.

À la suite de l'incident, le Bureau du Calgary a adopté de nouvelles procédures plus strictes. Les jeux de fiches et les lecteurs sont désormais conservés et utilisés dans une pièce sûre qui n'est jamais déverrouillée sans qu'il y ait quelqu'un à l'intérieur. Les employés doivent inscrire dans un registre les fiches qu'ils veulent utiliser; on les sort du jeu de fiches, puis on remet le jeu dans l'armoire verrouillable. En outre, on utilise des mesures de contrôle radiocales pour la destruction des vieilles fiches.

Ces nouvelles mesures rendent inutiles les recommandations que le Commissariat aurait pu faire à Revenu Canada pour l'amener à resserrer la sécurité dans ses services de Calgary. Toutefois, le Commissaire a recommandé au Ministère d'ordonner à ses autres bureaux de modifier leurs méthodes d'entreposage et de traitement des microfiches de façon à respecter la Loi sur la protection des renseignements personnels et la nouvelle politique du gouvernement sur la sécurité. En outre, il a répété plusieurs des recommandations qu'il avait faites après le vol de microfiches qui avait eu lieu au bureau de Toronto du Ministère (Rapport annuel 1986-1987) :

* les employés devraient être sensibilisés à leur obligation de protéger les renseignements personnels en vertu de la Loi sur la protection des renseignements personnels;

* les microfiches devraient être protégées plus étroitement encore que les dossiers sur support papier et

* le personnel ne devrait avoir accès aux microfiches que s'il en a vraiment besoin.

L'entreprise de camionnage responsable a cherché les caisses pendant près de deux semaines avant de les retrouver dans son entrepôt. Les caisses ne semblaient pas avoir été ouvertes, mais l'incident aurait pu être évité si l'on avait pris des mesures de sécurité normales.

Le second incident est le suivant : le Service correctionnel du Canada a perdu plus de 30 caisses de vieux dossiers de détenus pendant leur transport jusqu'au Centre des dossiers des Archives nationales, en Colombie-Britannique.

La plupart des employés traitent la sécurité en matière d'information comme le fief des agents de sécurité ou des spécialistes de l'information de gestion. Or, la formation que ces gens ont reçue les pousse à définir la sécurité dans le contexte de « l'intérêt national » et non de la vie privée des particuliers. Souvent, ils ne savent pas comment réagir à la cote « protégé », qu'on applique désormais à tous les renseignements personnels qui ne sont pas d'intérêt national.

Le Conseil du Trésor, le Centre de sécurité des télécommunications, la GRC et le Commissariat ont fait de grands efforts pour sensibiliser les employés à la protection des renseignements personnels, rarement considérés jusqu'à présent comme étant vulnérables, du point de vue de la sécurité. Grâce à des échanges réguliers, les quatre organismes ont défini des niveaux de protection correspondant au caractère délicat des renseignements personnels. Ces niveaux seront inclus dans la nouvelle politique du gouvernement sur la sécurité. La publication et l'application de ce nouveau document de principe devraient aider les ministères et organismes à appliquer des normes de sécurité pour tous les renseignements désignés.

Le Commissariat a enquêté cette année sur la perte d'un document et joué les observateurs dans l'enquête qu'un ministère a menée sur des dossiers perdus. L'enquête a porté sur la perte de microfiches d'impôt au bureau de district de Revenu Canada (impôt) à Calgary. En octobre 1988, Revenu Canada a informé le Commissaire qu'il avait perdu 38 feuilles d'un jeu de microfiches. Ces feuilles contenaient des renseignements permettant d'identifier des employeurs (grâce à un code numérique) et leurs employés (noms de famille, initiales, numéros d'assurance sociale, revenus, pensions, contributions à l'assurance chômage et autres retenues à la source). Chaque feuille pouvait contenir des données sur plus de 8 000 personnes.

L'enquête a commencé à l'administration centrale du Ministère, à Ottawa. Les enquêteurs ont retracé la procédure de production et d'envoi des jeux de microfiches, ce qui les a convaincus que le jeu était arrivé intact à destination.

Ensuite, les enquêteurs ont suivi la piste des fiches jusqu'au bureau de district de Calgary. Une fois que le jeu a été ouvert et que les fiches ont été comptées, elles ont été mises dans un boîtier auquel environ 150 employés avaient accès pendant la journée. La nuit, les fiches étaient gardées sous clé dans une armoire, mais les clés étaient dans un tiroir de bureau non verrouillé. Le matin, le premier employé qui avait besoin des fiches pouvait déverrouiller l'armoire et mettre les fiches dans le boîtier. On n'a jamais pu savoir qui avait sorti le jeu de l'armoire le jour où la perte a été constatée. Les 38 fiches n'ont jamais été retrouvées.

Vérification du travail des vérificateurs

Bien entendu, six vérificateurs ne sauraient en si peu de temps enquêter sur tous les organismes gouvernementaux assujettis à la *Loi sur la protection des renseignements personnels*. Par conséquent, le Commissaire a toujours pressé les vérificateurs internes des ministères et organismes de veiller à la protection de la vie privée. L'année écoulée a révélé des efforts encouragés en ce sens.

Emploi et Immigration Canada a bien répondu à l'appel. Après avoir consulté le Commissariat, le Bureau de la vérification interne de la Commission a entrepris un examen de la façon dont EIC traite les renseignements personnels. Le Commissariat a par la suite étudié les documents de travail des vérificateurs internes pour déterminer le niveau de confiance qu'ils pouvaient attribuer à la vérification. L'examen a révélé un travail de qualité tout à fait professionnel, que le Commissaire peut accepter avec une confiance égale à celle qu'il accorderait à un rapport de ses propres vérificateurs. (Les constatations sont résumées plus loin.)

Constatations

Certaines constatations valent pour tous les ministères et organismes visés. Par exemple, rares sont les employés d'autres services que ceux de l'accès à l'information et de la protection de la vie privée qui connaissent leurs droits en vertu de la *Loi sur la protection des renseignements personnels*, ou qui comprennent leurs responsabilités pour la collecte, la conservation, l'usage, la divulgation et le retrait des renseignements personnels.

Les vérifications ont fait ressortir la nécessité d'une politique applicable à l'ensemble de l'administration fédérale et précisant qui devrait être autorisé à consulter les dossiers de renseignements personnels. Cette politique devrait tenir compte des subtilités de la *Loi sur la protection des renseignements personnels* et limiter la quantité de renseignements de ce genre dont les cadres ont besoin pour s'acquitter des exigences légitimes de leurs postes. La présentation actuelle de la plupart des dossiers du personnel fait qu'il est impossible de cloisonner les renseignements en fonction du principe du besoin de savoir.

Cette année encore, les vérificateurs ont constaté que certains dossiers contenant des renseignements personnels n'ont pas été identifiés et décrits correctement dans le *Répertoire de renseignements personnels*. De même, certains usages des renseignements personnels que l'institution considèrerait comme « compatibles » avec les fins auxquelles ils avaient été recueillis ne figuraient pas dans les descriptions du Répertoire.

En outre, ces renseignements sont généralement mal protégés. Les employés des services opérationnels (et même certains de ceux des services de sécurité) ne comprennent pas encore parfaitement la nouvelle politique gouvernementale sur la sécurité, et plus particulièrement ses dispositions portant sur la protection des renseignements personnels. Néanmoins, les vérificateurs n'ont trouvé aucun indice permettant de croire que la confidentialité de ces renseignements ait été menacée.

Direction générale de l'observation

Institutions ayant fait l'objet d'une vérification

Le Commissariat a choisi les organismes devant faire l'objet d'une vérification en fonction des risques globaux que ceux-ci présentaient, mesurés aussi objectivement que possible.

Les vérifications ont porté sur la Société canadienne des postes, le Secrétaire du Solliciteur général et Emploi et Immigration Canada, ainsi que sur des institutions de taille plus réduite, à savoir le ministère des Finances, la Commission d'appel des pensions et le Conseil des sciences du Canada.

Le Commissariat termine actuellement des vérifications dans les organismes suivants : La Commission de réforme du droit, Le Centre de recherches pour le développement international, la Commission d'examen des exportations de biens culturels, la Société pour l'expansion des exportations et la Société canadienne des brevets et d'exploitation Ltée.

Méthode de vérification

Les vérifications sont confiées à des équipes de deux à quatre enquêteurs qui visitent un certain nombre de services de l'administration centrale et plusieurs bureaux régionaux des ministères et organismes visés. Ils examinent un échantillon de dossiers prélevés au hasard dans certains fichiers et interrogent les cadres et les employés qui utilisent et gèrent ces dossiers.

La vérification porte sur les aspects suivants :

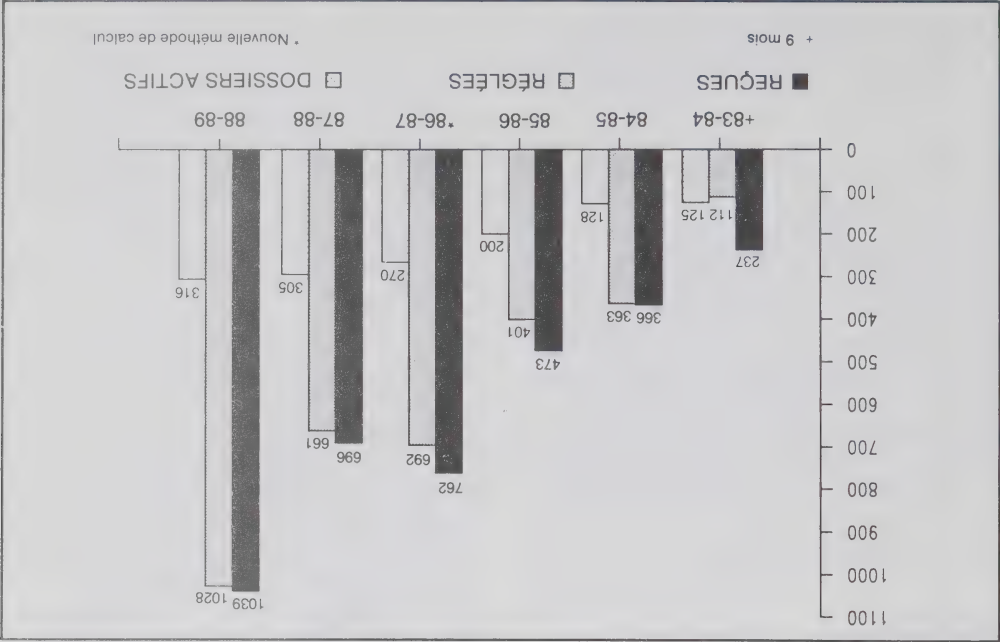
* la collecte, l'usage, la divulgation, la conservation, le retrait et la sécurité des renseignements personnels;

- * la qualité des lignes directrices internes et l'observation par le ministère ou l'organisme intéressé de la politique et des directives sur les renseignements personnels établies par l'organisme central;
- * l'exactitude et le caractère exhaustif du contenu du Répertoire de renseignements personnels du ministère ou de l'organisme;
- * la connaissance qu'a le personnel de la Loi sur la protection des renseignements personnels et de ses implications pour le traitement de ces renseignements;
- * l'accès des particuliers aux renseignements personnels les concernant;
- * la délégation des pouvoirs par le responsable du ministère ou de l'organisme.

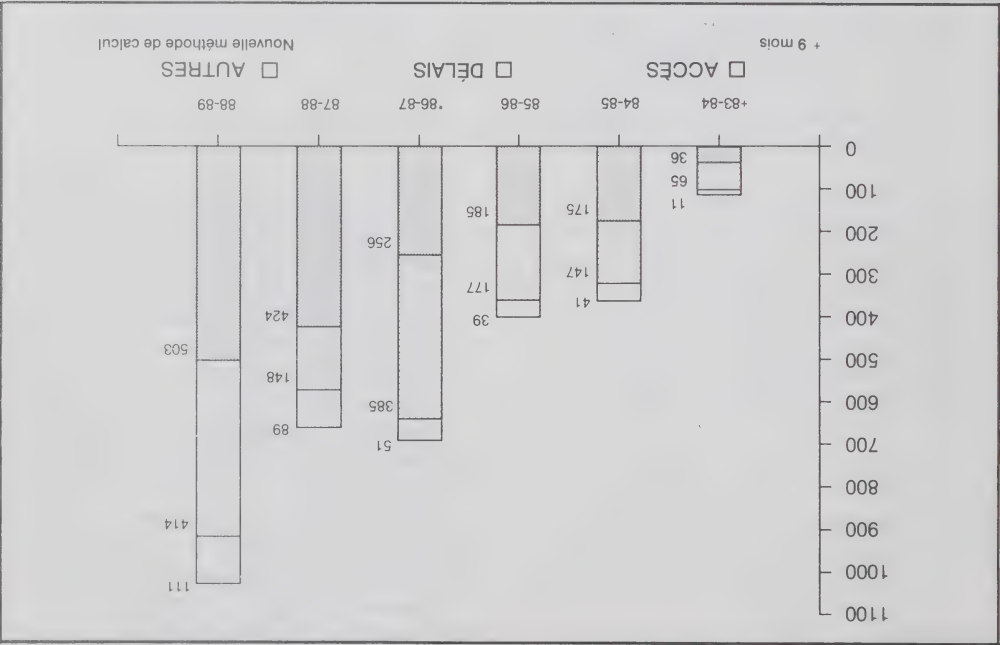
Une fois la vérification terminée, les enquêteurs parlent avec les cadres de leurs constatations, en insistant sur les lacunes relevées. Le ministère (ou l'organisme) reçoit d'abord un projet de rapport, puis un rapport final. Conformément à la pratique courante de vérification, les rapports ne portent que sur les points à corriger.

Enfin, 15 p. 100 des demandes portent sur des questions de protection de la vie privée dans le secteur provincial ou privé, qui ne sont pas du ressort du Commissariat. Par exemple, une Ontarienne a téléphoné au Commissariat pour savoir si la *Loi sur la protection des renseignements personnels* pouvait empêcher les autorités municipales de vendre leur liste d'électeurs à des entreprises ou à des particuliers. Le Commissariat n'a pas pu faire enquête, étant donné que les municipalités ne relèvent pas de la Loi. Elles ne seront d'ailleurs pas assujetties à la législation provinciale avant 1991. (Il est interdit de vendre les listes électorales fédérales.)

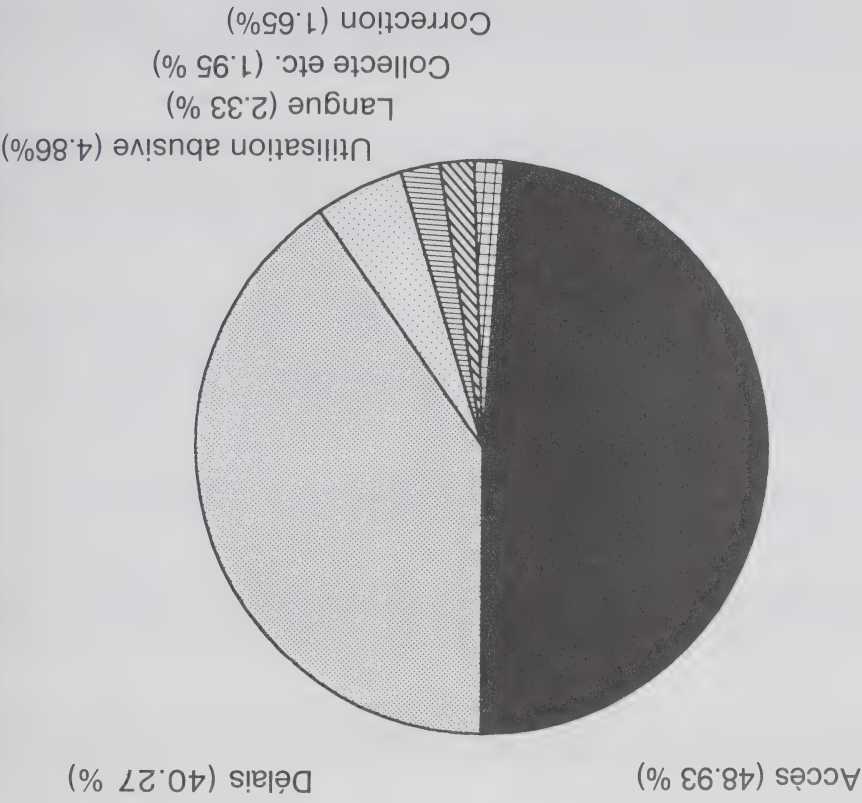
Nombre de dossiers 1983-1989



Plaintes réglées et motifs 1983-1989



Plaintes réglées par motifs 1988-1989



Plaintes régées par institution, motifs et résultats (suite)

Ministère	Nombre	Bien-fondée	Bien-fondée - Résolue	Non-fondée	Abandonnée
Consommation et Corporations Canada	1	0	0	1	0
Défense nationale	85	32	4	46	3
Emploi et Immigration Canada	68	24	13	28	3
Energie, Mines et Ressources Canada	2	1	1	0	0
Environnement Canada	3	0	0	0	3
Gendarmerie royale du Canada	109	13	6	86	4
Justice Canada, Ministère de la Revenu Canada - Douanes et Accise	5	0	0	5	0
Revenu Canada - Impôt	15	5	1	9	0
Santé et Bien-être social Canada	37	11	0	21	5
Service canadien du renseignement de sécurité	18	3	5	8	2
Service correctionnel Canada	49	3	6	40	0
Société canadienne d'hypothèque et de logement	404	203	29	168	4
Société canadienne des ports	1	0	1	0	0
Société canadienne des postes	4	0	4	0	0
Société canadienne des postes	12	2	2	7	1
Solliciteur général Canada	22	0	0	22	0
Transports Canada	77	31	2	43	1
Travail Canada	5	0	0	5	0
Travaux publics Canada	2	0	0	2	0
TOTAL	1028	336	98	566	28

Plaintes réglées par institution, motifs et résultats

Ministère	Nombre	Bien-fondée	Bien-fondée - Résolue	Non-fondée	Abandonnée
Affaires des anciens combattants Canada	3	0	0	3	0
Affaires extérieures Canada	14	3	1	10	0
Affaires indiennes et du Nord Canada	1	0	1	0	0
Agriculture Canada	5	0	2	3	0
Archives nationales du Canada	15	1	0	14	0
Bureau de l'enquêteur correctionnel	1	0	1	0	0
Bureau de l'inspecteur général du service canadien du renseignement de sécurité	4	0	0	4	0
Bureau du Conseil privé	6	0	1	5	0
Bureau du Directeur général des élections	1	0	0	1	0
Comité de surveillance des activités de renseignement de sécurité	4	0	0	4	0
Commissariat aux langues officielles	3	0	0	3	0
Commission canadienne des droits de la personne	11	0	2	9	0
Commission de la Fonction publique	8	0	4	3	1
Commission nationale des libérations conditionnelles	30	3	11	15	1
Communications, Ministère des	2	1	1	0	0
Conseil canadien des relations de travail	1	0	0	1	0

Le nombre de demandes a presque doublé cette année, le Commissariat en a reçu 2041, comparativement à 1248 l'an dernier. Une agente à temps plein reçoit la majorité des appels et son système efficace d'inscription des demandes fait paraître l'augmentation plus importante qu'elle ne l'est en réalité. Auparavant, on ne comptait tout simplement pas certaines demandes; le personnel y répondait sans prendre le temps de les consigner.

Les questions sont très variées. Elles peuvent être aussi simples que de vouloir savoir à quel ministère ou organisme s'adresser pour avoir accès à des renseignements personnels (environ 8 p. 100 des demandes).

D'autres demandes peuvent prendre un temps fou, mais se révéler très enrichissantes, comme l'appel d'un député sur un questionnaire détaillé que les auxiliaires temporaires de la Société des postes ont dû remplir avant d'être embauchés pour livrer du courrier publicitaire. Après discussion avec le Commissariat, la Société a cessé d'utiliser ce questionnaire. Les demandes de renseignements sur l'utilisation et l'interprétation de la Loi sur la protection des renseignements personnels reprennent 46 p. 100 du total.

Les questions et les plaintes sur l'utilisation du NAS (numéro d'assurance sociale) se sont multipliées cette année, jusqu'à concurrence de 21 p. 100 du total des demandes de renseignements. Cette augmentation est largement imputable à une modification de la Loi de l'impôt sur le revenu qui oblige les particuliers à donner leur NAS à leurs institutions financières. Certains des gens qui ont communiqué avec le Commissariat se sont indignés de la contradiction qu'ils trouvaient entre la nouvelle poli-

tique gouvernementale de restriction de l'utilisation du NAS et cette obligation de le donner aux banques, compagnies de fiducie, coopératives de crédit, caisses populaires et maisons de courtoisie. Les agents du Commissariat ont dû leur préciser qu'ils étaient aussi tenus de le donner aux agents d'immobiliers qui mettent des chèques de dépôt en banque et aux agents d'assurance.

D'autres personnes étaient mécontentes de ce qu'elles considéraient comme le « secret » qui avait entouré l'introduction de cette nouvelle obligation. En fait, comme nous l'avons précisé, les modifications à la Loi de l'impôt sur le revenu ont été adoptées conformément à la procédure parlementaire normale. Les députés n'ont pas soulevé de questions sur cette nouvelle obligation de produire le NAS, et la presse n'en n'a pas fait état. La plupart des gens qui ont communiqué avec le Commissariat à ce sujet ont été mis au courant de cette nouvelle obligation et de l'amende qu'ils devraient payer à défaut de donner leur NAS quand ils ont acheté leur nouvelle émission d'obligations d'épargne du Canada ou qu'ils sont allés à la banque... et ils n'ont pas été très contents.

Environ 10 p. 100 des gens qui demandaient des renseignements déplorent que certaines institutions fédérales ne soient pas assujetties à la Loi sur la protection des renseignements personnels. (Il s'agit souvent de sociétés d'État, comme Air Canada et le Canadien National.) Un certain nombre de sociétés d'État devraient être assujetties à la Loi en 1989.

Pourtant, la jurisprudence est claire : le secret professionnel d'un avocat s'applique aux communications entre les parties et aux documents créés ou obtenus expressément dans le contexte d'un litige. Les documents qu'un client confie à un conseiller juridique ne sont pas tous protégés par le secret professionnel. Par exemple, les faits obtenus d'autres sources, sans l'être pour l'avocat ou par celui-ci, ne sont pas protégés.

Le Commissaire a informé Transports Canada qu'il considérait que c'était donner à la notion de secret professionnel une extension inacceptable. Il a recommandé que les documents contenus dans le dossier de grief soient divulgués, ce qui a amené le Ministère à divulguer une partie des renseignements. Le Commissaire a alors proposé à la plaignante de porter elle-même sa cause à la Cour fédérale. Elle a accepté, et le Commissaire en a informé Transports Canada, qui avait entre-temps reçu un avis du ministère de la Justice, et qui a décidé de divulguer les renseignements demandés. Le Commissaire a jugé la plainte bien fondée.

les interférences électromagnétiques s'intensifient, le Ministère considère ce contrôle comme un élément important de la gestion du spectre. Il estime en outre qu'il n'est pas bon de permettre à des particuliers d'utiliser anonymement une ressource commune.

Par ailleurs, en sa qualité de membre de l'Union internationale des télécommunications, le Ministère est tenu d'offrir au public l'accès aux noms, aux adresses et aux indicatifs d'appel des opérateurs, en vertu de deux articles du règlement international, qui portent sur les enquêtes dans les cas d'interférence, la communication entre les opérateurs et leur perfectionnement personnel.

De plus, le Ministère divulgue des renseignements sur les licences pour permettre aux amateurs de communiquer entre eux, ce qui comprend la vérification des indicatifs et d'autres détails techniques. Ces mesures aident les opérateurs à s'acquitter des responsabilités qui leur incombent en vertu du Règlement général sur la radio, lequel les oblige à confirmer si un contact est un amateur licencié. Enfin, le Ministère est tenu de divulguer les noms et le statut (licencié ou pas) des amateurs utilisant des systèmes partagés (tels que des satellites), qui sont financés et maintenus par la collectivité des amateurs.

D'un autre côté, le Ministère a reconnu que les opérateurs ne tenaient pas tous à se joindre à des clubs, à se porter volontaires pour assurer des services de communication en cas d'urgence ou à figurer dans des répertoires. Néanmoins, il estime que les amateurs ne peuvent pas se soustraire à leur responsabilité de rendre publique leur utilisation du spectre.

Le Commissaire a accepté les arguments bien étouffés que le Ministère lui a présentés pour justifier la divulgation des renseignements, en soulignant que les opérateurs peuvent demander aux éditeurs de répertoire du secteur privé de ne pas publier les renseignements qui les concernent. Il a jugé la plainte non fondée.

Le secret professionnel d'un avocat va loin!

Une femme mêlée à une poursuite pour congédiement injuste intentée contre Transports Canada avait demandé les renseignements qui la concernaient dans les 20 fichiers ordinaires des employés du Ministère. Elle a porté plainte au Commissaire, en disant que la réponse avait tardé à venir et qu'il manquait des renseignements.

L'enquête a révélé que 14 des fichiers ne contenaient pas de renseignements sur l'intéressée. Il était aussi évident que Transports Canada n'avait pas communiqué certains renseignements qui figuraient dans le dossier de grief de la plaignante, soit parce qu'ils concernaient quelqu'un d'autre, soit parce que le Ministère considérait qu'ils étaient protégés par le secret professionnel d'un avocat.

L'enquêteur a découvert que Transports Canada avait refusé de communiquer sa demande d'opinion juridique, l'opinion juridique elle-même et toute la documentation pertinente. Le Ministère avait conservé cette documentation, qui fait normalement partie du dossier de grief, pour obtenir une opinion juridique. Selon lui, une fois que ces renseignements ont été joints à une demande de conseils juridiques, ils sont protégés par le secret professionnel d'un avocat.

On divulgue des renseignements personnels sur les opérateurs radio amateurs

Un opérateur radio amateur s'est plaint que le ministère des Communications avait divulgué des renseignements personnels sur les opérateurs radio amateurs à des associations d'opérateurs amateurs et à des éditeurs qui s'en servent pour produire des répertoires des opérateurs licenciés. Le ministère a une base de données dans laquelle il conserve les noms et les adresses de ces opérateurs.

Le plaignant s'opposait à la divulgation de ces renseignements personnels, parce qu'il ne voulait pas devenir la cible des expéditeurs de courrier indésirable ou de voleurs en quête de matériel radio coûteux.

Saisi de la plainte, le Ministère a suspendu la communication des renseignements jusqu'à ce que le Commissaire rende sa décision. Résultat : un barrage d'appels et de lettres d'opérateurs au Ministère et au Commissariat.

L'enquête a révélé que cette divulgation est une question complexe. Les représentants du Ministère ont expliqué au Commissaire pourquoi ils la considéraient comme compatible avec les fins auxquelles les renseignements ont été recueillis.

Le Ministère est chargé de la gestion du spectre radioélectrique, une ressource publique limitée. Les personnes qui réussissent l'examen d'agrément se voient assigner un indicatif d'appel lorsqu'ils reçoivent leur licence. Comme les opérateurs sont connus publiquement, ils peuvent s'autocorriger, étant donné que les abus et les erreurs des amateurs peuvent nuire aux autres transmissions radio. À mesure qu'on approche du point de saturation et que

Une semaine avant de porter plainte, la femme avait demandé à la Cour fédérale de déclarer que Revenu Canada ne pouvait pas se servir des renseignements contenus dans les déclarations d'impôt, sauf aux fins autorisées par la Loi de l'impôt sur le revenu. Elle avait plus particulièrement soutenu que ses déclarations d'impôt ne devaient pas être citées en preuve dans une audience sur son congédiement.

Le Commissaire a reporté sa décision jusqu'après celle de la Cour. Le juge a reconnu que, en sa qualité d'employeur, Revenu Canada n'a pas le droit de se servir des déclarations d'impôt des particuliers pour l'administration du personnel.

La Loi sur la protection des renseignements personnels autorise le Ministère à utiliser les renseignements personnels uniquement aux fins auxquelles ils ont été recueillis, « sous réserve d'autres lois du Parlement ». Étant donné que ce n'est pas le cas ici, et que, d'après la Cour, l'utilisation des renseignements n'était pas justifiée en vertu de la Loi de l'impôt sur le revenu, le Commissaire a conclu que la plainte était bien fondée.

Cela ne signifie pas que Revenu Canada ne peut pas imposer de mesures disciplinaires aux employés couvres disciplinaires au employes couvres d'évasion fiscale. Le Ministère devrait tout simplement porter plainte contre ces employés, comme il le ferait dans le cas de n'importe quel autre soupçonné d'évasion fiscale, puis prendre des mesures disciplinaires appropriées s'il sont jugés coupables.

Plaintes par motifs et résultats

1028	566	98	336	28	TOTAL
3	3	0	0	0	Conservation/Retrait
17	12	2	1	2	Collecte
0	0	0	0	0	Répertoire
24	23	0	1	0	Langue
414	79	14	317	4	Délais
17	10	6	1	0	Correction/annotation
50	29	7	8	6	Utilisation/Divulgation
503	410	69	8	16	Accès
Total	Rejetée	Bien fondée Résolue	Bien fondée	Abandon- née	Motifs

anonymes, au besoin, pour confirmer ou infirmer l'existence d'un absentéisme chronique déjà constaté.

Les lignes directrices imposent aussi des restrictions quant aux personnes qui peuvent consulter et comparer les registres, et à qui ils peuvent être divulgués.

Interdiction d'utiliser les dossiers d'impôt pour des motifs disciplinaires

Une vérificatrice de l'impôt congédiée pour avoir falsifié ses déclarations d'impôt sur le revenu s'est plainte au Commissaire que Revenu Canada (impôt) avait enfreint la Loi de l'impôt sur le revenu et la Loi sur la protection des renseignements personnels en se servant de ses déclarations d'impôt pour des motifs disciplinaires.

d'opter pour une méthode d'enquête qui perturberait bien davantage la vie privée des employés.

Le Commissaire n'a pas été convaincu par cet argument. Il a eu du mal à accepter l'idée que des comparaisons discrétionnaires des registres des pré-sences des conjoints, des autres membres de la famille et des partenaires de golf des employés fassent partie intégrante de la gestion des pré-sences. Il a conclu qu'accepter le bien-fondé d'une démarche comme celle-là équivaldrait à établir des distinctions injustes contre les employés dont les parents ou les amis travaillaient aussi pour la Société des postes. Il a donc recommandé à la Société de mettre fin à ces comparaisons.

La Société n'était pas d'accord, mais elle était disposée à négocier une solution. Après d'autres discussions, elle a adopté des lignes directrices pertinentes. Désormais, elle continuera d'examiner les registres des présences des employés, mais ne les comparera avec d'autres que pour produire des renseignements

Non-divulgation du nom d'un informateur dans une affaire d'impôt

Une femme de Winnipeg s'était plainte à l'Institut manitobain des comptables agréés que son ancien comptable agréé avait commis une faute professionnelle. L'institut a fait enquête et il a demandé à Revenu Canada (impôt), au nom de la plaignante, de lui communiquer sa déclaration d'impôt sur le revenu.

Revenu Canada a refusé de divulguer certains renseignements, soit parce qu'ils concernaient une autre personne, soit parce que leur divulgation aurait nui à l'application de la Loi de l'impôt sur le revenu.

L'avocat intéressé a porté plainte au Commissaire. L'enquête a révélé qu'une partie des renseignements concernait effective-ment quelqu'un d'autre, de sorte que leur non-divulgation était parfaitement légitime. Le reste des renseignements portaient sur une source confidentielle. Le Commissaire a reconnu que la divul-gation de ces renseignements risquait de nuire à l'application de la Loi de l'impôt sur le revenu. Toutefois, il a ajouté qu'on pourrait maintenir que l'intérêt public aurait été mieux servi par une divulgation des renseignements en question. Néanmoins, la Loi sur la protection des renseignements personnels donne au ministre en cause le droit de décider, d'après le Commissaire, Revenu Canada n'a pas abusé de ses pouvoirs en refusant de divulguer les renseignements, et il a jugé la plainte non fondée.

L'employeur comparait les registres de congés de maladie

Une femme a demandé au Commissariat si la Société canadienne des postes (son employeur et celui de son mari) pouvait se servir de son registre des présences pour enquêter sur l'absence de son mari. Le dossier de la femme avait été communiqué à un superviseur dont elle ne relève pas, et le mari avait trouvé une des fiches de présence de sa femme dans son propre dossier. L'enquête a dû déterminer s'il était admissible que la Société compare les registres des présences du couple pour vérifier les présences du mari. La Société estimait que cette utilisation des renseignements était compatible avec la raison pour laquelle ils avaient été recueillis, puisqu'elle voulait s'assurer que les employés se servaient de leurs congés conformément à la convention collective. Selon elle, quand la direction soupçonne qu'il y a des abus, il est « naturel » qu'elle examine les registres des présences, même de deux personnes ou davantage, au besoin.

Le Commissaire a informé la Société qu'il comprenait ses raisons d'agir ainsi, mais que son geste lui semblait entrefreindre la Loi sur la protection des renseignements personnels. Il a invité la Société à lui répondre avant de rendre sa décision finale. La Société a répondu que la comparai-son des dossiers facilitait le contrôle des absences et des présences dans les cas où la direction soupçonne que les employés sont de connivence pour abuser de leurs congés. Selon elle, faute de pouvoir comparer les dossiers pour confirmer le caractère frauduleux des demandes, elle serait forcée

Le Commissaire a trouvé ces arguments convaincants et il a jugé la plainte non fondée.

Les requérants n'ont pas accès aux noms des personnes consultées sur leur compte

Certains candidats à des postes de la GRC et certains anciens membres de la Gendarmerie avaient demandé des renseignements tirés de leurs dossiers de sécurité. Ils se sont plaints quand la GRC ne leur a pas communiqué les noms et les commentaires des personnes impliquées au cours des enquêtes de sécurité.

La GRC fait des enquêtes de sécurité plus poussées dans le cas des policiers que dans celui des simples fonctionnaires. En effet, les policiers ont le pouvoir d'arrêter des gens et de porter des armes à feu, de sorte que leur température et leur caractère ont une importance toute particulière. Bref, la GRC a déclaré qu'elle devait protéger ses sources pour être sûre de leur franchise.

Après avoir discuté des plaintes avec l'enquêteur, la GRC a consenti à examiner les renseignements en question. Elle a conclu que les commentaires de ses sources pouvaient être divulgués, mais elle n'a pas voulu révéler leur nom ou d'autres détails grâce auxquels on aurait pu les identifier, afin de protéger l'intégrité des enquêtes.

Le Commissaire a accepté cette solution; il a jugé les plaintes bien fondées, mais résolues.

Un dossier d'hôpital datant de la

Deuxième Guerre mondiale a disparu

En dépit des efforts des Archives nationales, un citoyen de la Colombie-Britannique n'a pas obtenu tous les renseignements qu'il voulait du fichier des Dossiers médicaux de la Seconde Guerre mondiale.

Le plaignant a déclaré au Commissaire que les Archives lui avaient envoyé des renseignements, mais que les documents sur son séjour dans un hôpital au cours des années 1940 manquaient. Il s'agissait notamment d'un formulaire qu'il avait été obligé de signer pour s'engager à ne pas demander de pension militaire.

À la demande d'un enquêteur, les Archives ont fait des recherches dans d'autres fichiers, mais sans succès. Elles ont trouvé les dossiers de l'hôpital (qui n'existe plus), mais pas ceux de la période du traitement du plaignant.

L'enquêteur s'est alors adressé au ministère des Anciens combattants, qui a lui aussi fait des recherches, sans réussir à trouver les dossiers manquants.

Le Commissaire a conclu que les dossiers étaient introuvables et que les Archives avaient fait de leur mieux. Il a jugé la plainte non fondée.

renseignements personnels, on lui a remboursé les 25 \$.

La plainte était fondée.

Les évaluations de rendement doivent être conservées cinq ans

Lorsqu'un plaignant a déclaré qu'un ministère conservait trop longtemps les évaluations de rendement de ses employés, il a suscité des discussions entre Revenu Canada (Douanes et Accise), les Archives nationales, le Conseil du Trésor et le Commissaire à la protection de la vie privée.

Le plaignant a déclaré au Commissaire que Douanes et Accise conservait les évaluations de rendement plus de trois ans, malgré la période indiquée dans le *Répertoire de renseignements personnels*. La période de conservation des évaluations est fixée par les Archives nationales, de concert avec le Conseil du Trésor. Toutefois, Douanes et Accise considérait qu'il n'était pas tenu de respecter cette durée et qu'il n'y avait pas matière à plainte. Par contre, le Conseil du Trésor considérait la période comme obligatoire.

Le Commissaire a accepté d'étudier la question. Après enquête, il a été confirmé que Douanes et Accise avait bien conservé les évaluations du plaignant (comme toutes les autres) pendant plus de trois ans. Après des consultations avec Douanes et Accise, le Conseil du Trésor et les Archives nationales, l'enquêteur a constaté que le Conseil du Trésor avait porté la période de conservation à cinq ans, mais que Douanes et Accise n'avait pas été mis au courant. Après discussion, le Ministère a conclu que l'esprit de la politique du Conseil du Trésor était clair, et il a accepté de respecter la période de cinq ans.

Les résultats des tests doivent être interprétés par des spécialistes

Une avocate qui se préparait à plaider en appel avait demandé des renseignements sur son client contenus dans deux fichiers du Service correctionnel du Canada (SCC). Elle a porté plainte quand celui-ci ne lui a pas communiqué les renseignements. L'enquête a révélé qu'une grande partie des renseignements contenus dans le fichier des dossiers médicaux des contrevenants est fournie à titre confidentiel par une province, de sorte que le SCC est tenu par la Loi de ne pas les divulguer. L'enquêteur a donc proposé à l'avocate de demander les renseignements en invoquant la loi provinciale.

Le SCC avait aussi déclaré inconsultables les données brutes des tests psychologiques conservées dans son fichier de données psychologiques, en disant que la divulgation de ces renseignements n'aurait pas bien servi les intérêts du détenu, parce que les résultats bruts auraient pu être mal interprétés par des profanes.

D'après un psychologue du SCC, le test est protégé par le droit d'auteur, et les psychologues n'ont pas le droit d'en donner de copie. En outre, si les questions, les réponses et les résultats étaient rendus publics, les tests ne seraient plus valides, particulièrement dans un milieu fermé comme un établissement pénitencier. De plus, les résultats des examens peuvent varier d'un jour à l'autre selon l'état de santé ou l'humeur des sujets. Là encore, les profanes risquent de mal interpréter les fluctuations et les résultats ponctuels. On a conseillé à l'avocate de retenir les services d'un psychologue agréé auquel les renseignements demandés auraient pu être communiqués, en sa qualité de témoin expert.

Par conséquent, la GRC n'avait rien discuté qui n'ait déjà été divulgué au procès.

La plainte a été rejetée, parce que la Loi permet aux institutions gouvernementales de communiquer des renseignements personnels exigés par subpoena.

Il ne coûte rien d'invoquer la Loi sur la protection des renseignements personnels

Un homme âgé s'est plaint qu'on lui ait facturé 25 \$ pour s'être prévalu de la *Loi sur la protection des renseignements personnels*. Il avait lu l'information sur la façon d'invoquer la Loi dans le *Guide des programmes et des services fédéraux pour les aîné(e)s*, une publication de Santé et Bien-être social Canada. Par la suite, il a demandé son dossier d'emploi aux Archives nationales et son dossier d'immigration à Emploi et Immigration Canada (EIC).

Les Archives nationales ont fait suivre sa demande à son ancien employeur, le plaignant a reçu les renseignements demandés peu de temps après. Toutefois, EIC lui a facturé 25 \$ pour ses papiers d'immigration. Étant donné qu'il n'était pas question de frais dans le Guide, l'intéressé a écrit à Santé et Bien-être social Canada pour leur demander de le préciser à l'avenir.

Un enquêteur a constaté que le personnel d'EIC avait tout simplement mal interprété la demande. Les personnes âgées ont souvent besoin de copies certifiées de leurs documents d'entrée au pays pour étayer leurs demandes de pension. Or, EIC facture ce service. S'étant rendu compte que le plaignant ne voulait pas de copies certifiées, mais simplement consulter le dossier en vertu de la *Loi sur la protection des*

Le Commissaire a reconnu que les Affaires extérieures avaient besoin de ces renseignements, mais était-il clairement indiqué sur le formulaire qu'ils n'étaient indispensables que dans les trois cas susmentionnés? Les Affaires extérieures ont consenti à expliquer la question dans un nouveau formulaire.

Le Commissaire a rejeté l'idée qu'on portait atteinte à la vie privée des gens en exigeant que les garants connaissent les détails de leur état civil. En effet, les garants ne sont pas simplement témoins de la signature des requérants; ils attestent que les renseignements fournis sont exacts, au meilleur de leur connaissance.

Le Commissaire a déclaré que, « puisqu'un passeport permet à son porteur d'entrer au Canada de plein droit, l'obligation de divulguer ces renseignements aux garants ne peut être considérée comme une exigence déraisonnable ».

Il a donc jugé la plainte non fondée.

La GRC peut communiquer des renseignements exigés par subpoena

Un avocat mêlé à une poursuite mettant en cause une compagnie d'assurance s'est plaint que la GRC avait donné à l'avocat de la compagnie une copie de la déclaration de son client à la police, sans son consentement.

La GRC a expliqué qu'elle avait parlé de cette partie du dossier avec l'avocat de la compagnie, mais qu'elle ne lui avait ni donné une copie du document, ni permis d'en consulter une. Toutefois, les renseignements en question avaient été exigés par subpoena au cours du procès au pénal d'un autre individu. La GRC a produit les renseignements exigés par ce subpoena; ils faisaient donc partie des dossiers du tribunal.

EIC peut obtenir des renseignements médicaux détaillés sur les prestataires de l'assurance-chômage

Un Ontarien s'est plaint de la quantité de renseignements médicaux que la Commission d'emploi et d'immigration du Canada a recueillis quand il a réclamé des prestations d'assurance-chômage pour raisons médicales.

Le plaignant exerçait des fonctions modifiées au moment de sa mise en disponibilité, parce qu'il avait été blessé. Il a communiqué à EIC des renseignements provenant de son médecin, qui avait précisé sa période de convalescence. Sa demande de prestations a été acceptée. Une semaine plus tard, un spécialiste a prolongé la période de convalescence du plaignant parce que sa blessure guérissait mal. Par la suite, la période de convalescence a été de nouveau prolongée. Chaque fois, le plaignant a informé EIC. Après la deuxième prolongation, EIC a demandé au médecin de remplir un formulaire. Toutefois, les renseignements obtenus ne lui ont pas paru satisfaisants. Le médecin s'est donc vu réclamer plus de détails. Il a rempli le formulaire avec réticence, parce que ces détails étaient d'après lui protégés par le secret professionnel.

L'enquête a révélé que les deux médecins avaient fourni des renseignements contradictoires. En pareil cas, EIC a le droit d'exiger un diagnostic pour pouvoir régler la demande. Le Commissaire a conclu que les responsables d'EIC avaient agi avec prudence, conformément au règlement de l'assurance-chômage, en obtenant une corroboration des renseignements reçus. Il a considéré que la plainte n'était pas bien fondée.

Les données d'état civil sont nécessaires pour l'obtention d'un passeport

Un homme d'Ottawa s'est plaint d'avoir dû révéler son état civil actuel et passé à la personne qui s'était portée garante de sa demande de passeport. En outre, il a dit s'inquiéter de ce que les Affaires étrangères avaient recueilli trop de renseignements dans sa demande.

Les gens qui demandent un passeport doivent révéler s'ils sont mariés ou s'ils l'ont déjà été. On explique dans le formulaire que ces détails sont nécessaires pour établir l'identité, la citoyenneté ou la garde des enfants. Toutefois, l'enquête a révélé que l'information n'est indispensable que dans trois cas :

- * quand le nom de famille qui figure sur le passeport a changé après le mariage de la personne (il s'agit soit du nom de famille du conjoint, soit d'une combinaison du nom de famille de la personne et de celui du conjoint);
- * quand le nom des enfants est inscrit dans le passeport, (les détails fournis contribuent à la détermination de la garde légale);

* quand la personne qui demande le passeport est une femme mariée à un homme qui n'était pas sujet britannique avant le 1^{er} janvier 1947. La femme peut avoir cessé, suite à son mariage, d'être sujette britannique et, en application des lois en vigueur à l'époque, citoyenne canadienne.

Dans tous les autres cas, les examinateurs des demandes de passeport peuvent s'abstenir de tenir compte des renseignements sur l'état civil.

Bien fondée. Il y a eu infraction de la Loi, et il n'a pas été possible d'y remédier, soit parce que les documents étaient introuvables ou déjà détruits, soit parce que le délai était dépassé. On dit aussi qu'une plainte est bien fondée quand le requérant s'est vu refuser l'accès qu'il demandait et que le Commissaire a menacé d'avoir recours aux tribunaux pour obtenir la divulgation des renseignements en question.

Abandonnée. Le plaignant a retiré la plainte (souvent parce que le problème a été résolu avant le début de l'enquête), ou bien il n'a pas répondu aux appels ou aux lettres de suivi.

**Origine des plaintes réglées
par province et territoire**

Terre-Neuve	3
Ile-du-Prince-Edouard	35
Nouvelle-Ecosse	17
Nouveau-Brunswick	165
Québec	240
Région de la Capitale nationale	
Québec	4
Région de la Capitale nationale	
Ontario	53
Ontario	200
Manitoba	21
Saskatchewan	96
Alberta	57
Colombie-Britannique	134
Territoires du Nord-Ouest	1
Yukon	0
Hors Canada	2
Total	1028

Direction générale des plaintes

L'étonnante augmentation de 20 p. 100 du nombre des plaintes déposées en 1988-1989 (1 050, comparativement à 691 l'année précédente) est difficile à expliquer. Peut-être reflète-t-elle simplement un retour à la tendance établie depuis le début, à savoir une augmentation annuelle de 10 p. 100, ce qui ferait de la baisse de 1987-1988 une aberration largement compensée cette année par l'augmentation massive de la charge de travail. Quoi qu'il en soit, rien ne laisse entendre qu'il faut imputer l'augmentation à une résistance croissante à l'esprit ou à la lettre de la Loi.

L'augmentation globale du nombre de plaintes se double d'une prolifération des plaintes portant sur la lenteur avec laquelle les ministères et organismes répondent aux demandes. C'est devant, car le Commissaire avait espéré que le problème des retards s'éliminerait de lui-même à mesure que les institutions prendraient de l'expérience. En fait, le Commissariat a enquêté sur près de 400 plaintes au sujet de retards, dont 250 contre le Service correctionnel du Canada, en raison de l'augmentation marquée du nombre de demandes adressées à cet organisme.

Néanmoins, malgré l'augmentation substantielle du nombre de plaintes reçues pendant l'année, le Commissaire et ses collaborateurs se sont efforcés de régler les 296 affaires reportées de l'année dernier. À la fin de l'exercice, il n'en restait plus que quatre en souffrance. Les enquêteurs ont fermé 1 028 dossiers pendant l'année, ce qui représente une augmentation de 56 p. 100 par rapport à 1987-1988. La Direction générale continue à réduire la période d'enquête. La nouvelle norme est d'en moyenne trois mois et d'au plus six mois. À la fin de 1988-1989, 94 p. 100 des dossiers de plaintes étaient actifs depuis moins de six mois.

Question de statistiques... les noms changent, les notions restent

La terminologie utilisée pour décrire le règlement des plaintes a été modifiée par rapport à celle des années précédentes, afin que les ministères et organismes puissent utiliser une terminologie uniforme dans leurs rapports statistiques au Conseil du Trésor et au Commissariat. Après des discussions avec le Conseil du Trésor et toutes les autres parties, la terminologie suivante a été établie :

Non fondée (auparavant « rejetée »)

Bien fondée — résolue (auparavant « justifiée »). Après négociation, le Commissaire est arrivé à ce qu'il considère comme une solution raisonnable. Cela ne signifie pas toujours que le plaignant est entièrement satisfait.

Cette accélération s'explique partiellement du fait que la Direction générale compte trois nouveaux postes d'agents, obtenus en prévision du moment où les sociétés d'État seront assujetties à la Loi. À la fin de l'année, ce n'était pas encore fait, de sorte que les nouveaux enquêteurs ont pu aider le Commissariat à absorber le flot de nouvelles plaintes. Comme l'effectif de la Direction générale est désormais complet, le Commissariat a confiance qu'il pourra continuer à respecter les nouvelles normes, au moins jusqu'à ce que les sociétés d'État entrent dans la danse.

Il faut donc surveiller de près tout ce qui accompagne les chèques du gouvernement.

Le Commissaire a entrepris des pour-
parlers avec le Conseil du Trésor en
vue de l'établissement de lignes direc-
trices grâce auxquelles les envois géné-
raux du gouvernement respectent la Loi.

Par exemple, le gouvernement a envoyé dans une enveloppe adressée aux 9 millions de prestataires des allocations familiales, des pensions de vieillesse et du Régime de pensions du Canada de l'information sur l'Accord de libre-échange canado-américain. En outre, il a envoyé et il envoie encore aux fonctionnaires des chèques de paye accompagnés d'annonces les invitant à acheter des obligations d'épargne du Canada et à contribuer à Centraide. Manifestement, il y a là des risques de conflit. Dans sa politique de communauté très logique, le gouvernement enjoint aux ministères et aux organismes d'informer le public de leurs activités. Les obligations d'épargne du Canada sont essentielles au financement des activités gouvernementales, et les personnes désireuses d'en acheter aiment manifestement être informées de l'émission des obligations et de la méthode de retenue automatique des paiements. De même, Centraide est largement tributaire des contributions des fonctionnaires, qui sont grandement facilitées par le système de retenue à la source.

Le principe posé par la Loi est pourtant clair : les renseignements recueillis pour une raison donnée ne peuvent pas l'être pour une autre.

Il y aura dans ce contexte des cas d'application de la Loi difficiles, pour lesquels il faudra beaucoup de jugement. Le Commissaire ne tient pas du tout à empêcher Centraide d'accomplir sa noble mission. Par contre, il tient beaucoup à empêcher le gouvernement de se servir de ses envois pour faire de la politique. Qu'il émane du gouvernement ou pas, le courrier indésirable est toujours indésirable.

Qu'est-ce qu'il y a avec le chèque?

Les listes de distribution postale : tout le monde comprend leurs implications pour la protection des renseignements personnels dans le secteur privé. Cela dit, bien peu d'organismes publics ou d'entreprises privées ont des listes de distribution aussi importantes et aussi à jour que le gouvernement fédéral.

Songez aux trois listes suivantes, par exemple :

— la liste des employés du gouvernement (y compris les membres des Forces armées et de la GRC), c'est-à-dire 350 000 personnes;

— la liste des prestataires des allocations familiales, des pensions de vieillesse et du Régime de pensions du Canada, soit environ 5,5 millions de noms et d'adresses;

— la liste de l'impôt sur le revenu (environ 17 millions de personnes).

Ces trois listes seraient une véritable mine d'or pour les expéditeurs postaux. D'ailleurs, certains les ont déjà demandées sans vergogne.

Ainsi, une maison de publication a demandé à Santé et Bien-être social Canada de lui fournir la liste de tous les prestataires du Régime de pensions du Canada et de toutes les personnes désireuses d'y adhérer. Elle voulait leur envoyer une brochure publicitaire offrant des services juridiques à tous ceux qui éprouvent des difficultés à cet égard.

Le gouvernement fédéral n'a pas le droit de vendre ou de donner ses listes de distribution, mais encore faut-il voir comment il les utilise lui-même... Les ministères et organismes fédéraux savent très bien qu'avec les enveloppes de leurs chèques, ils ont un moyen économique de communiquer avec leur clientèle. Le coût d'un ajout dans ces enveloppes est infime par rapport à celui d'une campagne de publicité, et le public cible est atteint avec une efficacité inégalée. En fait, ce serait un excellent moyen de vanter les bienfaits de la *Loi sur la protection des renseignements personnels* (« Savez-vous à quelle protection vous avez droit pour votre vie privée? »)

Les prestataires des allocations familiales et des pensions ont l'habitude de trouver des avis dans l'enveloppe de leur chèque mensuel. Est-ce une atteinte à leur vie privée?

Pas du tout, à condition que les renseignements communiqués soient directement liés au mandat du ministère au nom duquel le chèque est émis. Ainsi, Santé et Bien-être social Canada peut fort bien informer les retraités d'un changement de leurs prestations ou rappeler aux parents de faire vacciner leurs enfants en temps voulu.

Les risques d'abus sont néanmoins omniprésents. Le Conseil du Trésor s'en est rendu compte, tout à son honneur. Il oblige donc les ministères à obtenir son autorisation pour mettre des avis quelconques dans leurs envois ordinaires. La fiche de route de l'administration fédérale est généralement bonne, mais en dépit d'un suivi plus serré que jamais, 5 des 50 envois de l'an dernier n'avaient rien à voir avec la raison d'être initiale de la liste de distribution en cause.

Pour chaque demande d'accès reçue, le SCRS décide à quel fichier (010 ou 015) verser les renseignements recueillis par l'ancien Service de sécurité de la GRC. Il semble que ce soit la seule façon pratique de procéder jusqu'à ce que tous les dossiers qui ne répondent pas aux critères de collecte de la Loi sur le Service canadien du renseignement de sécurité aient été retirés.

Le Commissaire est heureux de pouvoir déclarer que le SCRS compte accélérer son examen et son retrait des vieux dossiers. Au cours des deux prochaines années, il devrait en avoir examiné et retiré deux fois plus qu'il ne l'a fait depuis cinq ans. Le Commissaire applaudit à cette initiative, mais il estime que le procédé devrait être suivi par un observateur indépendant, pour que toute l'information qui n'est pas « strictement nécessaire », aux termes de l'article 12 de la Loi sur le Service canadien du renseignement de sécurité, soit bel et bien retirée plutôt que simplement recylée sous une autre forme.

L'inspecteur général (en vertu des articles 30 et 31 de la Loi sur le Service canadien du renseignement de sécurité), le comité de surveillance des activités de renseignement de sécurité (en vertu de l'article 40 de ladite loi) et le Commissaire (en vertu de l'article 37 de la Loi sur la protection des renseignements personnels) semblent tous avoir le pouvoir et la responsabilité nécessaires pour assurer cette inspection indépendante.

Au cours des prochains mois, le Commissaire consultera les parties intéressées afin de déterminer les moyens d'assurer ce suivi du retrait des dossiers en évitant les dédoublements d'efforts.

SCRS a examinés avant de décider de les retirer. Il est réconfortant de constater qu'après examen, le SCRS a conservé moins de 100 dossiers. Cela dit, des milliers et des milliers de dossiers ne passeront pas par les déchiqueteuses avant des années.

En outre, les vieux dossiers de la GRC ont créé d'autres problèmes au SCRS. Comme il y est autorisé en vertu de la *Loi sur la protection des renseignements personnels*, celui-ci s'abstient de confirmer ou de nier l'existence de renseignements ayant conservé leur utilité pour lui. Les renseignements de ce genre sont conservés dans le fichier SRS/P-PU-010. Le SCRS ne veut pas non plus confirmer ou nier le fait qu'il n'existe pas de renseignements quand un requérant présente une demande d'accès à ce fichier en vertu de la *Loi sur la protection des renseignements personnels*. Le Commissaire et la Cour fédérale ont reconnu que ce qu'on appelle « l'effet de mosaïque » oblige le SCRS à adopter cette approche.

Néanmoins, le SCRS confirme l'existence de certains renseignements personnels recueillis par l'ancien Service de sécurité de la GRC. Les vieux renseignements de ce type, qui ont perdu leur caractère délicat, sont conservés dans le fichier SRS/P-PU-015. Leur existence est confirmée, et ils sont communiqués aux requérants sous réserve des exemptions expresses prévues dans la *Loi sur la protection des renseignements personnels*. Il n'a pas été possible au Commissaire de s'entendre avec le SCRS sur des lignes directrices définissant les renseignements « moins critiques », en dépit de la bonne volonté manifeste dont le SCRS a fait preuve en réponse aux préoccupations soulevées par le Commissaire dans son dernier rapport annuel.

Une autre collection de renseignements personnels très délicats a continué de préoccuper le Commissaire depuis l'an dernier : il s'agit des dossiers dont le Service canadien du renseignement de sécurité (SCRS) a hérité de l'ancien Service de sécurité de la GRC. Depuis que la définition des « menaces envers la sécurité du Canada » a été précisée, une grande partie de l'information contenue dans ces dossiers ne répond pas aux critères de collecte prévus par la *Loi sur le Service canadien du renseignement de sécurité*, du moins d'après le comité de surveillance des activités de renseignement de sécurité.

Bref, le SCRS se trouve par conséquent dans une situation fautive, étant donné qu'il est le gardien de renseignements personnels qu'il n'aurait pas le droit de recueillir en vertu de son mandat actuel. La solution paraît bien simple : il suffit de retirer les vieux dossiers!

Le SCRS a créé un service qu'il a chargé d'étudier les dossiers, d'en tirer les renseignements qui continuent de présenter de l'intérêt pour lui et d'éliminer le reste. Malheureusement, le procédé est très lent; en outre, certains des dossiers ont été « séquestrés », tandis que d'autres ont fait l'objet de règles spéciales régissant l'accès interne aux dossiers et leur utilisation par le personnel. Le SCRS et les Archives nationales se sont lancés dans des consultations afin de déterminer les renseignements à archiver et les conditions applicables en pareil cas.

Les déchiqueteuses ont pourtant bien servi! Depuis la levée du moratoire sur la destruction des dossiers qui avait été imposé en 1985, après l'intervention de la Commission Deschênes sur les criminels de guerre, on a retiré environ 120 000 dossiers du Service de sécurité, dont 67 000 que la GRC avait déjà prévu de détruire, et 53 000 que le

Il faut souligner tout particulièrement la valeur du travail du Centre de sécurité des systèmes du Centre de la sécurité des télécommunications, créé en août 1988 pour accroître la compétence en sécurité informatique de la GRC et du MDN et pour offrir au gouvernement du Canada de nouvelles possibilités d'évaluation des produits de sécurité pour les ordinateurs et les réseaux. La Loi sur la protection des renseignements personnels est l'un des éléments qui incite le Canada à se donner ses propres critères d'évaluation de la sécurité informatique. En effet, le gouvernement reconnaît que, même si c'est la protection des renseignements touchant la sécurité nationale qui pose les difficultés techniques les plus ardues, les problèmes les plus fréquents sont liés à la nécessité de protéger les renseignements personnels détenus par le gouvernement. Le Commissaire est heureux de cette initiative, et c'est avec plaisir qu'il envisage un échange durable d'information et d'idées avec le Centre de sécurité des systèmes.

« La sécurité consiste à protéger l'ordinateur de l'intervention humaine, la protection de la vie privée, c'est l'inverse. »

Robert P. Bigelow, dans *Computer Law and Security Report*, mars-avril 1989

Ce serait bien trop simple ! Dans les bureaux hautement automatisés, la sécurité informatique est essentielle pour protéger le personnel des autres, et c'est peut-être le but ultime des défenseurs de la vie privée.

Dans le monde décentralisé du traitement des données que nous connaissons, un système informatique absolument sûr est un idéal impossible. Aujourd'hui, les spécialistes de la sécurité informatique parlent de systèmes « fiables » plutôt que « sûrs ». (Belle réflexion sur notre société, ce mot « fiable » qui véhicule une certaine méfiance !)

Les systèmes d'information de gestion (SIG) sortent à peine de l'adolescence et, depuis le milieu de la dernière décennie, l'ordinateur est devenu partie intégrante de l'administration gouvernementale, grâce à ses nombreux talents : il est capable de traitement multiple, de manipulation de fichiers énormes, de transmission de données sur de grandes distances en quelques secondes et d'ouverture des ressources d'information à de nombreux utilisateurs.

De nos jours, il n'est plus rare de trouver dans un bureau gouvernemental des postes de travail polyvalents reliés à un ordinateur central ou à un réseau d'ordinateurs, en partageant consciemment ou inconsciemment les données, voire dans certains cas les logiciels.

Au cours de la dernière année, le Commissariat s'est intéressé au labyrinthe de la sécurité informatique, cet univers déroutant qui a une terminologie et une technologie bien à lui. La panoplie des ennemis internes des systèmes informatiques est étrange : saucissons, pièges, « bombes » à retardement, chevaux de Troie et vers, tout y est. Les armes de ceux qui s'attaquent aux ordinateurs de l'extérieur sont tout aussi exotiques, ce sont des virus, des perturbations préméditées, des communications et des explorations illlicites, des croisements de réseaux et des décodages frauduleux.

Ceux qui cherchent la parade sont aussi « colorés ». Aux États-Unis, le ministère de la Défense publie ses normes de sécurité dans le « Livre orange » et les explique dans le « Livre jaune ». La sécurité des systèmes d'établissement de réseaux fait l'objet du « Livre framboise », et ainsi de suite.

Le monde du SIG pose d'énormes problèmes de sécurité face auxquels le Commissariat commence à peine à acquiescer la compétence nécessaire pour définir les difficultés et pour proposer des solutions logiques et pratiques. Au cours de l'année à venir, il insistera particulièrement sur la sécurité des systèmes de TED, dans ses vérifications régulières des institutions gouvernementales.

Pour que la protection de la vie privée ait un sens dans les années 1990 et au-delà, il nous faudra prendre grand soin de veiller à ce qu'on impose des contrôles efficaces contre les méthodes nouvelles — et plus intrusives que jamais — de collecte de l'information. Pourtant, les années 1980 tirent à leur fin, et il semble bien que nos dirigeants ne penchent pas dans ce sens-là.

Certains hauts fonctionnaires et autres personnes influentes qui ont témoigné à l'Enquête Dubin se sont dits très favorables à l'idée d'obliger les athlètes subventionnés par le gouvernement fédéral à subir des analyses d'urine aléatoires à l'improviste. Il y a bien sûr de bons arguments pour justifier une mesure pareille, mais ce qui est inquiétant, c'est qu'une politique gouvernementale, même dans un secteur précis et avec le consentement tacite des athlètes, semble faire fi d'une notion fondamentale pour la vie privée de chacun, à savoir la présomption d'innocence. La nécessité d'empêcher une intrusion dans la vie privée des gens à moins qu'on puisse raisonnablement soupçonner un méfait précis a été clairement établie par la Cour suprême, dans le contexte de la Charte canadienne des droits et libertés. Le principe a toujours été maintenu, sauf dans des cas d'exception, pour protéger la vie humaine, par exemple en utilisant l'alcooltest à l'im-

provisé le long des routes.

Néanmoins, dans le cas des athlètes, la fierté nationale offensée semble large-ment suffire à justifier le rejet d'un principe fondamental de la liberté. Si nous pouvons accepter les intrusions nécessaires dans le cas des athlètes, et peut-être le juge Dubin conclura-t-il que nous le pouvons, ne sera-t-il pas plus facile pour les employeurs de justifier leurs intrusions biologiques chez leurs employés actuels ou éventuels? L'enquête sur l'utilisation des drogues par les athlètes risque d'avoir sur notre philosophie de la protection de la vie privée des retombées qui débordront les stades, et plus encore les vestiaires.

Si le Commissaire souligne dans ses rapports annuels son inquiétude à l'égard du couplage informatique, autrement dit de la comparaison de bases de données différentes afin d'en tirer des profils de certaines personnes, c'est que la méthode équivaut à une perquisition et à une saisie de dossiers sans motifs raisonnables. C'est précisément pour la même raison qu'il continuera à suivre de près l'évolution des programmes d'analyse biotechnologique, afin de protéger la vie privée des innocents.

Dans l'ensemble, le gouvernement obtient son information sur les citoyens par des méthodes traditionnelles : des enquêtes, des formulaires, des lettres, voire l'observation directe. Pourtant, il est possible d'abuser même de ces méthodes, au point de porter grave-mment atteinte à la vie privée. Toutefois, il y a plus grave : les techniques de collecte « intrusives » se répandent de plus en plus.

Ces techniques, dont certaines sont très récentes, permettent de tirer des renseignements sur les gens directement de leur organisme. C'est le cas de l'alcootest et du polygraphe. Les analyses d'urine et de sang et le codage génétique sont en train de s'imposer comme moyens de révéler des secrets personnels ignorés parfois même des premiers intéressés.

Les milieux policiers sont passés maîtres dans l'utilisation de ces méthodes, qui sont toutefois de plus en plus souvent utilisées comme techniques d'évaluation hors du contexte pénal. Seriez-vous un employé loyal et digne de confiance? Risquez-vous d'avoir des comportements dangereux pour autrui? Avez-vous enfreint les règles régissant une activité qui vous intéresse? Êtes-vous génétiquement prédisposé à certaines maladies, ou vulnérable à certains styles de personnalité? Les employeurs du secteur public et du secteur privé sont tentés d'avoir recours à la biochimie pour répondre à ces questions.

Ainsi, le ministère de la Défense nationale fait des analyses de sang des employés désireux de suivre des cours sur la défense aux États-Unis, afin de vérifier s'ils sont porteurs du VIH. Le SCRS se sert d'un polygraphe pour vérifier si les candidats à des postes dans son organisation sont loyaux et dignes de confiance. Enfin, Transports Canada s'interroge sur l'opportunité de soumettre les travailleurs des transports à des analyses d'urine pour voir s'ils consomment des drogues illégales.

Sports Canada fait des pressions pour que les athlètes qu'il subventionne subissent des analyses d'urine pour y détecter la présence de substances interdites (mais pas nécessairement illégales) capables d'améliorer les performances des athlètes, et donc de leur donner un avantage injuste. La GRC se sert de matériaux génétiques à des fins d'identification, et elle doit mettre sur pied un répertoire national d'identification génétique analogue à celui des empreintes digitales qu'elle conserve déjà. En outre, les chercheurs poursuivent leurs travaux en vue de l'établissement de profils physiques et comportementaux des individus grâce à des analyses de l'ADN.

À en croire un commentateur, nous passerions de l'ère de l'information à l'ère biotechnologique. La transition exposerait la protection de notre vie privée à des risques comme nous n'en avons jamais connus.

Ces recommandations ont été conçues de façon à refléter un compromis convenable entre la nécessité de la protection des renseignements personnels et les besoins légitimes de certaines institutions gouvernementales. Si la compréhension que le public a du SIDA et de sa transmission change — et s'il change aussi d'attitude — les recommandations pourraient être remises en question, tout comme si l'on découvrait un vaccin ou une cure. Le rapport ne l'a pas caché :

« Cette terrible maladie a spontanément fait surgir dans l'humanité l'espoir que soit rapidement découvert un remède ou un vaccin efficace. Mais l'espoir n'allège en rien les responsabilités que doit maintenir l'assumer la société. Les principes énoncés dans le présent document dans le but de répondre aux problèmes que suscite, sur le plan de la protection de la vie privée, le traitement des renseignements personnels concernant les personnes séropositives et sidatiques n'apportent peut-être guère de réconfort à long terme, mais au moins, ils ont le mérite d'humaniser la réaction de la société. Pour le moment, peut-être ne pouvons-nous rien faire de mieux. »

loin. Heureusement, les partisans de la protection des renseignements personnels sont d'accord à ce sujet avec les plus éclairés des médecins : il faudrait toujours que les gens se soumettent à des examens de dépistage du SIDA de leur plein gré, en bénéficiant de conseils avant et après les examens.

Le gouvernement du Canada a un rôle important à jouer pour faire en sorte que le SIDA soit traité avec sensibilité dans les milieux de travail. Le rapport du Commissaire invite instamment le Conseil du Trésor, en sa qualité de plus important employeur au Canada, à formuler une politique exhaustive sur le SIDA dans les milieux de travail.

Le caractère confidentiel des renseignements personnels est partie intégrante de la politique du milieu de travail proposée par l'Organisation mondiale de la santé. L'employé ne devrait pas être forcé de dire à l'employeur s'il est porteur ou pas du VIH, et il n'est pas nécessaire non plus qu'il le dise à ses collègues. Si l'employé communique de son plein gré des renseignements personnels liés au SIDA, il faudrait leur accorder une excellente protection et, avant son embauche, le futur employé ne devrait être soumis à aucun examen direct ou indirect (évaluation des comportements à risques ou questions au sujet des examens préalables) de dépistage du VIH. L'une des raisons que les gens donnent le plus souvent lorsqu'ils hésitent à subir volontairement des examens de dépistage des anticorps du VIH, c'est qu'ils craignent de ne pas pouvoir contrôler la mesure dans laquelle des tiers auront accès à cette information.

La Loi elle-même précise 13 cas dans lesquels les ministères peuvent communiquer des renseignements personnels à des tiers sans le consentement des intéressés. Compte tenu de la nature particulièrement délicate des renseignements liés au SIDA, *La Loi sur la protection des renseignements personnels* recommande qu'on applique une procédure très rigide avant de divulguer des renseignements de ce genre. Chose plus importante encore, la décision de divulguer quoi que ce soit du genre à des tiers devrait toujours être prise par le responsable de l'institution gouvernementale, en fonction des éléments suivants :

1. les raisons rendant la divulgation nécessaire;
 2. le préjudice que cette divulgation pourrait entraîner pour la ou les personnes intéressées;
 3. la capacité du requérant de garder le secret et
 4. la capacité du requérant d'utiliser les renseignements exclusivement aux fins pour lesquelles ils avaient été demandés initialement.
- Dans tous les cas, il devrait incomber au requérant de justifier la communication des renseignements sans le consentement de la ou des personnes intéressées.

Sur un autre front, comme il l'avait prom-
mis dans son rapport de l'année der-
nière, le Commissaire a préparé des
recommandations pour s'assurer que
les renseignements personnels sur le
SIDA seront traités par le gouvernement
fédéral conformément à l'esprit et à la
lettre de la Loi. Dans son rapport, inti-
tulé *Le SIDA et la Loi sur la protection
des renseignements personnels*, le
Commissaire confirme que la réaction
d'envergure nationale qui s'impose dans
le cas du SIDA est peut-être la question
de protection de la vie privée la plus
délicate et la plus émotive de notre
époque. Dans son rapport, le Commis-
saire recherche un équilibre fugace
entre la protection de l'intimité de ceux
qui souffrent du SIDA ou qui sont por-
teurs du VIH (le virus qui cause le SIDA)
et la divulgation nécessaire à la protec-
tion de leur entourage.

Par compassion pour les porteurs du

virus, il faut les protéger contre le trauma-
tisme qu'entraînerait une intrusion inutile

dans leur vie privée et une divulgation
de leur état. Apprendre qu'on est vic-

time du SIDA continue d'être un arrêt
de mort. En fait, d'après certains, être

porteur du VIH, c'est la mort prochaine.

Les réactions illogiques et extrémistes
du public et des gouvernements à

l'annonce que quelqu'un souffre du
SIDA ou qu'il est porteur du VIH peuvent

parfois modifier de façon très réelle les
conditions de l'appartenance d'une per-

sonne à la société, en limitant son accès
à l'école, au travail, aux soins médicaux,

voire à sa famille et à ses amis. En
fait-il davantage pour réclamer le plus

de respect possible pour la vie privée
des victimes?

Le Commissaire conclut dans son rap-
port que la vérification obligatoire des
anticorps du VIH pour des groupes
comme les fonctionnaires, les détenus
des pénitenciers fédéraux, les immi-
grants et les visiteurs à long terme au
Canada entrainerait la Loi. En effet,
celle-ci interdit la collecte de renseigne-
ments personnels qui ne sont pas liés
directement à un programme ou une
activité ressortissant au mandat législatif
d'une institution gouvernementale. Il se
fait qu'une vérification pareille n'est pas
un élément fondamental d'un programme
législatif actuel.

Bien sûr, le Parlement peut prévaloir
sur la Loi et donner au gouvernement le
pouvoir d'obliger certains groupes à
subir volontairement des examens de
dépistage des anticorps du VIH. Toute-
fois, les mesures de ce genre seraient
une réaction hystérique exagérée à la
prolifération du SIDA, du moins dans
l'état des connaissances actuelles de la
maladie.

Les avantages pour la santé publique
susceptibles de résulter d'une vérifica-
tion à si grande échelle sont pour le
moins douteux; les effets dévastateurs
de sa corollaire, l'intrusion dans la vie
privée des gens, l'emporteraient de

Ce n'était qu'un début. Le même disque au laser contient maintenant les coordonnées de chaque ménage, à un mètre près, sur une carte topographique du Canada, avec les noms des voisins, la circonscription électorale et la période d'occupation à l'adresse indiquée, en plus de 12 champs démographiques (vendus globalement par Statistique Canada), notamment sur le revenu, la langue officielle, la religion et le nombre d'enfants. Toute cette information fait partie du domaine public, mais dès qu'on y ajoute des renseignements sur les cartes de crédit ou sur les comptes bancaires, à supposer qu'on puisse les obtenir par des moyens honnêtes ou pas, on aboutit à un profil de la population à échelle aussi grande que systématique.

et encore au Pakistan).

Une entreprise a déjà transféré sur un disque au laser de 4,7 pouces les noms, adresses et numéros de téléphone de 7,9 millions des 8,5 millions de ménages canadiens. Le processus a été long et coûteux (au-delà de 1 million de dollars,

nuaire téléphonique.

ne nous touche de plus près qu'un an- données lisibles à la machine. Et rien (les mots mêmes sont menaçants) des la transformabilité infiniment accrues l'accessibilité, de la transférabilité et de particulièrement menacée en raison de La vie privée des consommateurs est traitement électronique des données. d'un support papier à des disques de numéros de téléphone sont transférés lorsque les noms, les adresses et les que la qualité des données se modifie Le Commissaire est intervenu parce

C'est un outil de rêve pour la commercialisation, mais un cauchemar pour la protection de la vie privée. L'information lisible à la machine peut être manipulée de toutes les façons imaginables pour le démarchage téléphonique ou postal. Et pourtant, cette utilisation-là serait virtuellement innocente. Les inscriptions du genre sont aussi un moyen de contrôle ou de suivi non seulement pour les spécialistes de la commercialisation, mais aussi pour les criminels et pour les organismes policiers.

Les abonnés du téléphone n'ont jamais imaginé, encore moins consenti à, une telle intrusion dans leur vie privée lorsque leur nom paraît dans le bottin téléphonique. Malheureusement, avec la technologie moderne, le danger est réel et imminent.

Vous voulez des données? Composez Bell!

Le Commissaire ne s'est pas contenté d'être un simple spectateur et d'évaluer la prestation du gouvernement. Il s'est lancé dans la partie, lorsqu'il a appris en novembre dernier que le Conseil de la radiotélévision et des télécommunications canadiennes se demandait s'il fallait autoriser Bell Canada à vendre la base de données et aux pages jaunes de pages blanches et aux pages jaunes de l'annuaire téléphonique, sous forme lisible à la machine. Le Conseil se demandait à qui et sous quelles conditions Bell aurait pu le faire. La demande n'emanait pas de la compagnie de téléphone, mais bien d'entreprises qui convoitaient sa base de données. Quel bel exemple de l'intensité des pressions exercées en vue d'échapper à grande échelle de renseignements personnels informatisés! (C'est aussi un bon exemple de la façon dont un organisme de réglementation intelligent devrait être conscient des enjeux.)

Avec une remarquable retenue, le CRTC a déclaré que le fait de communiquer ces renseignements sous forme lisible à la machine risquait d'accroître les in-quiétudes quant à la protection des renseignements personnels sur les consommateurs. Il s'agit bien d'accroître les inquiétudes! Même s'il n'y a rien de plus public qu'un annuaire téléphonique, les clients de Bell ont de bonnes raisons de s'inquiéter. Le Commissaire les a exposées dans une intervention officielle, en demandant au CRTC de ne pas obliger Bell Canada à offrir la base de données de ses annuaires à tous les acheteurs éventuels.

Ce sont là des solutions de désespoir inspirées par des visions cauchemardesques. Il y a sûrement un moyen terme. Les règles de respect volontaire de la vie privée, telles que les lignes directrices de l'OCDE, sont parfaitement logiques et, pour peu qu'on les applique, elles semblent promettre des garanties raisonnables. Néanmoins, le moment est venu pour le gouvernement d'imposer dans ce domaine un régime de volontariat analogue à celui de l'armée. Les entreprises réglementées par le gouvernement fédéral, qui auraient dû être assujetties à la Loi d'après la recommandation unanime du Comité du Parlement, devraient être le point de départ de cette démarche. En plus de poursuivre avec une énergie accrue une stratégie de coopération avec les provinces afin d'encourager le respect volontaire des lignes directrices de l'OCDE, le gouvernement du Canada devrait s'attaquer au secteur privé qu'il ouvre un second front pour la protection des renseignements personnels. Il devrait enjoindre au secteur privé de se donner des codes de protection de la vie privée efficaces, dans un délai précis, puis d'en informer clients et employés (qui seront ravis) sous peine de se voir imposer une loi exécutoire.

Les partisans d'une loi sur la protection des renseignements personnels dans le secteur privé ont raison sur un point : les invitations aimables n'ont pas eu grand effet. Il reste qu'il est préférable d'augmenter un peu la pression plutôt que d'échafauder un lourd appareil de protection législative de la vie privée.

Le professeur Flaherty, un spécialiste de réputation internationale de la législation sur la protection de la vie privée et des données, s'est exprimé en termes quasi apocalyptiques :

« Les bases de données informatisées d'aujourd'hui rendent possible un contrôle relativement intégré des citoyens des pays occidentaux. C'est la prolifération de ces fichiers d'information publics et privés, plutôt que l'existence de l'un ou l'autre d'entre eux, qui est le véritable défi pour les protecteurs de la vie privée. Nous devons absolument penser aux implications de pratiques de surveillance comme celle-là pour la protection des droits de la personne. En Amérique du Nord, l'application de la technologie de l'information progresse à un rythme de loin plus rapide que l'évolution de la réglementation et des mesures de contrôle. »

Être privé de son pouvoir de contrôler ce que le monde sait de soi est humiliant et déshumanisant. Ceux qui réclament leur droit à la vie privée n'ont rien du marginal ou du dillettante. Ils vont au cœur même de l'intégrité et de la dignité de l'être humain et du genre de société que nous souhaitons tous. C'est là que la protection de la vie privée prend toute son importance. Et la protection de la vie privée est particulièrement critique dans les relations entre les citoyens et leurs gouvernements, étant donné que l'État a d'énormes pouvoirs d'extraction et d'utilisation des renseignements personnels.

à appliquer.

Pourtant, la conclusion d'un concordat pour la protection de la vie privée dans le monde de l'entreprisisme est en passe de devenir presque aussi indispensable. En effet, même quand nous donnons volontairement des renseignements personnels (et ce n'est souvent pas le cas, par exemple pour une demande de crédit), des règles claires s'imposent si nous voulons que l'individu conserve au moins un certain contrôle sur les utilisations qu'on en fera.

Un autre spécialiste de la protection de la vie privée, le professeur James Rule, de l'Université de l'État de New York, déclarait récemment que le meilleur moyen d'assurer la protection des renseignements personnels consisterait sur l'utilisation commerciale de l'information personnelle le concernant. Cette information ne pourrait ni être vendue, ni donnée en contrepartie d'un avantage quelconque sans l'autorisation de l'intéressé. C'est un concept ingénieux et fascinant, voire logique, mais il est bien peu réaliste, et manifestement impossible

La demande de renseignements personnels poursuit sa croissance exponentielle. Arthur Miller, qui enseigne le droit à Harvard, affirme qu'il ne suffit pas pour voler d'avoir un billet en main quand on se présente à l'aéroport. Pour les transporteurs aériens, les passagers n'existent pas à moins que le code numérique voulu apparaisse à l'écran d'affichage; ils ne sont qu'une version tridimensionnelle de l'information affichée. Et M. Miller de poursuivre :

« Nous avons fini par comprendre qu'il est impossible de souscrire une assurance, d'obtenir du crédit, de décrocher certains emplois ou d'avoir accès à certains avantages gouvernementaux sans faire approuver nos dossiers; nous savons que des gens passent nos dossiers au peigne fin. Nous ne savons pas qui sont ces gens, ni où ils sont. Nous ne savons pas non plus quels sont les critères décisionnels. »

« Ce n'est pas simplement un système de réservation de billets d'avion. L'ordinateur a mon nom, mon numéro de téléphone, le numéro de ma carte de crédit et le nom des gens avec qui je prends l'avion. Il sait si j'ai fait réserver une chambre d'hôtel ou loué une voiture par son intermédiaire. C'est un véritable dossier. »

Il y a bien d'autres dossiers : pas moyen de dormir dans un lit Sheraton à moins d'être reconnu par l'ordinateur. Nous finissons par nous rendre compte que notre vie est contrôlée par une banque de données après l'autre, au gré des ordinateurs.

C'est le prix de la commodité et de l'efficacité, et personne n'irait proposer qu'on détruise les ordinateurs. Néanmoins, il faudrait qu'on adopte et qu'on respecte des règles fondamentales de traitement des énormes quantités de renseignements personnels collectés par tout un chacun. Le danger, c'est que les collections de données peuvent servir, sur simple pression d'un bouton, à prendre des décisions cruciales pour nous. Arthur Miller le dit bien :

Qui décide? Sommes-nous maîtres des renseignements personnels qui nous concernent? Devons-nous céder le pas aux collecteurs et aux marchands de renseignements personnels, armés de leurs merveilleuses machines? En devrions-nous pas perdre la moindre parcelle de notre humanité. Autrement, nous serions les esclaves de nos machines, et les sociétés de l'information seraient devenues des « sociétés surveillées », réalisant ainsi la sombre prophétie du professeur David Flaherty, de l'Université Western.

Par conséquent, pour la plupart des gens, y compris le Commissaire, l'autoréglementation l'emporte sur la réglementation par le gouvernement. Les lois de la deuxième génération sur la protection des données qui ont été récemment adoptées (dans les 12 derniers mois, en Irlande, en Australie et au Japon) se rapprochent bien plus du modèle canadien que des lois de la première génération qui régissaient le secteur privé en Suède et en France. Il reste qu'en l'absence de preuves plus concluantes de l'efficacité de l'autoréglementation, les partisans des codes de protection volontaire des données auront de plus en plus de mal à défendre leur point de vue.

effet, le ministre des Affaires extérieures ne semble pas avoir obtenu de résultats probants lorsqu'il a demandé aux grandes entreprises d'appliquer ces lignes directrices dans leur exploitation.

Le gouvernement fédéral a rencontré à deux reprises les gouvernements provinciaux pour élaborer des stratégies propres à inciter le secteur privé à appliquer les lignes directrices. Toutefois, les parties ne semblent pas s'être entendues sur les secteurs d'activité visés ou sur les stratégies elles-mêmes.

Le gouvernement a besoin d'une approche plus énergique. C'est le strict minimum depuis qu'il a rejeté la recommandation unanime du Comité permanent de la Justice et du Solliciteur général, qui voulait que tout le secteur privé de compétence fédérale soit assujéti à la Loi.

Cette recommandation n'a pas été acceptée (et le Commissaire était d'accord sur ce point), parce que l'autoréglementation semblait alors la méthode optimale : la déréglementation est à la mode. Les quelques expériences d'autoréglementation n'ont pas révélé d'abus endémiques ni même très fréquents. En outre, on peut se demander s'il est possible de concevoir une *Loi sur la protection des renseignements personnels* applicable à toute la gamme des entreprises privées, des banques aux cablodistributeurs. À l'âge du micro-ordinateur, il est imaginable qu'on puisse appliquer la réglementation de façon parfaitement étanche. D'ailleurs, s'il fallait que le Commissariat soit une gigantesque organisation employant des régiments entiers d'enquêteurs, plus personne ne voudrait en entendre parler.

D'autres démocraties occidentales ont reconnu la nécessité de protéger par des codes les impressionnantes quantités de renseignements personnelles emmagasinées dans les ordinateurs des transporteurs aériens. Si British Airways peut s'accommoder de la législation sur la protection des données du Royaume-Uni, Air Canada devrait pouvoir s'accommoder de la Loi sur la protection des renseignements personnels.

Petro-Canada est une société d'État à 100 %, mais sa direction n'a pas voulu être assujettie à la Loi parce qu'elle craint que cela nuise à ses affaires.

Peut-être Petro-Canada aura-t-elle la vie plus facile si elle n'est pas tenue de communiquer à ses clients ou à ses locataires les dossiers de crédit qu'elle détient sur eux, comme elle devrait le faire en vertu de la Loi. Elle aurait d'ailleurs la vie bien plus facile si elle n'était pas obligée de satisfaire aux exigences des droits de la personne ou de la législation sur l'équité en matière d'emploi, mais il n'est pas question de l'en dispenser. La protection du droit à la vie privée des employés et des clients de Petro-Canada est pourtant au moins aussi importante.

Si des institutions aussi en vue qu'Air Canada et Petro-Canada étaient exemptées de la Loi, on pourrait considérer à juste titre que le gouvernement se soustrait à ses propres engagements. En effet, presque toutes les institutions publiques ou privées peuvent imaginer des raisons pour justifier d'être exemptées de lois à caractère réglementaire sur la protection de la vie privée ou sur d'autres principes.

Via Rail pourrait par exemple contester l'application de la Loi, à l'instar de la Société Radio-Canada. Il n'empêche que ces deux sociétés d'État y seront assujetties (bien qu'avec certaines dispositions spéciales de protection des activités journalistiques de la seconde). Utopisme, ce désir d'assujettir deux sociétés d'État à la Loi quand le secteur privé tout entier, qui comprend des entreprises réglementées par le gouvernement fédéral, échappe totalement à la Loi? Pourquoi s'inquiéter d'Air Canada quand les autres compagnies aériennes canadiennes volent paisiblement sans devoir respecter les contraintes de l'équité en matière d'information? Pourquoi insister pour que les clients de Petro-Canada bénéficient de la protection de la Loi tandis que ceux de leurs concurrents sont livrés à eux-mêmes? Bien sûr, exempter deux institutions de plus de la Loi — ou au contraire les y assujettir — n'aura pas grand effet sur la qualité globale de la protection de la vie privée au Canada, mais si le gouvernement n'insiste pas pour que ses créatures respectent ses règles, le secteur privé ne l'écouterait pas quand il l'invitera à adopter des codes comme les principes de protection des données de l'Organisation pour la coopération et le développement économiques (OCDE).

Et l'autoréglementation?

Dans ce contexte, les démarches du gouvernement fédéral pour encourager l'entreprise privée à respecter les lignes directrices de l'OCDE que le Canada a signées n'ont guère été efficaces. En

Bien sûr, il faut payer ses impôts. L'application de la nouvelle Loi a été remarquée par conséquent, dès que la déduction de 1 000 \$ pour les intérêts a été abolie. Il reste que les implications des nouvelles demandes de NAS — et de la peine imposée à ceux qui refusent de le donner — sont bien plus vastes que quiconque ne semble s'en être rendu compte. Il est vraiment dommage que personne n'ait pensé à se renseigner ou à expliquer la situation.

Si peu de temps après avoir annoncé son admirable politique de restriction de l'utilisation du NAS, le gouvernement autorise des milliers d'institutions du secteur privé (qu'on songe seulement au nombre de succursales bancaires!) à conserver de nouveaux dossiers avec le NAS comme code d'identification. Le fait que l'utilisation abusive du NAS soit frappée d'une amende de 5 000 \$ est une piètre consolation.

...et un autre

Dans *Les prochaines étapes*, le gouvernement s'est engagé à élargir le mandat de la Loi aux sociétés d'Etat fédérales et à leurs filiales. Cette mesure fera presque doubler le nombre d'institutions assujetties à la Loi et, chose plus importante encore, elle fera du gouvernement un véritable chef de file pour le secteur privé. Bref, en mettant en œuvre ces pratiques équitables en matière d'information, le gouvernement mettait de l'ordre dans ses affaires.

linguistiques....

Air Canada a été exemptée parce qu'elle n'est plus une société d'Etat à 100 % : le raisonnement est contestable, puisque le gouvernement continuera d'en être l'actionnaire majoritaire quoi qu'il arrive. Ce fait devrait à lui seul l'obliger à respecter son engagement original. En période de privatisation, ce serait imposer un principe dangereux que d'exempter des sociétés d'Etat de l'application d'une loi fédérale du seul fait que leur propriété est partagée. Jusqu'à présent, ce motif n'a pas suffi. D'ailleurs, Air Canada est toujours assujettie à la Loi *sur les langues officielles*, et elle le resterait probablement même si elle était complètement privatisée. La protection de la vie privée des clients et des employés d'Air Canada est sûrement aussi importante que celle de leurs droits linguistiques....

jetties à la Loi.

Comme de nombreuses sociétés d'Etat font directement concurrence à des entreprises privées, la décision du gouvernement de les assujettir à la Loi fait vraiment passer le message qu'à son avis, la protection des données peut être un atout, plutôt qu'un obstacle à la bonne conduite des affaires. La Société canadienne des postes doit respecter la Loi depuis cinq ans, et elle a constaté qu'elle pouvait fort bien mener ses affaires en dépit d'une concurrence intense. Il se peut donc fort bien que la grande majorité des sociétés d'Etat finissent par être assujetties à la Loi (des membres du Commissariat faisant partie d'un groupe de sensibilisation, sont allés rencontrer des représentants de 21 sociétés d'Etat), mais l'initiative du gouvernement a souffert de la lenteur du processus et surtout de deux omissions de taille. En effet, ni Air Canada, ni Petro-Canada ne figurent sur la liste des institutions qui seront assujetties à la Loi.

La complexité des modifications de la Loi de l'impôt sur le revenu est telle que cette nouvelle utilisation du NAS — et les répercussions qu'elle entraîne — ont échappé aux députés et sénateurs, à la presse, voire le Commissariat à la protection de la vie privée. Comment pouvait-on prévoir trouver dans cette Loi une disposition influant sur la protection de la vie privée? On voit à quel point la protection de la vie privée est vulnérable aux assauts les plus inattendus!

Pour la première fois, refuser de donner son NAS est une infraction punissable en vertu de la nouvelle Loi de l'impôt sur le revenu. Depuis le début, la loi et les règlements donnent aux institutions gouvernementales le pouvoir d'exiger les NAS, surtout pour des programmes sociaux comme l'assurance-chômage et les pensions. Sans numéro, il n'y a ni assurance, ni prestations. Désormais, à défaut de numéro, il y a une amende de 100 \$. (Ceux qui refuseront de payer l'amende écoperont-ils de deux jours de prison?)

C'est une autre première. Jusqu'à l'adoption de ces modifications à la Loi de l'impôt sur le revenu, les Canadiens n'étaient légalement tenus de donner leur NAS qu'au gouvernement fédéral. Maintenant, ils sont forcés de le donner aux banques, compagnies de fiducie, maisons de courtage, coopératives de crédit et caisses populaires chaque fois qu'ils font ce qui semble être un investissement portant intérêt. Bravo pour la société de l'ordinateur...

Un pas en arrière

En évitant les abus dans sa propre administration, le gouvernement fédéral a désormais une autorité morale accrue, en plus de son autorité légale, pour faire pression sur les autres paliers de gouvernement et sur le secteur privé. Si l'on continue à exiger la divulgation du NAS sans raison valable, il faudra manifestement adopter une loi restrictive, et ce ne serait que justice.

Trois mois seulement après l'annonce d'une politique extrêmement encourageante de limitation des utilisations du NAS, le Parlement a adopté des modifications à la Loi de l'impôt sur le revenu, dont l'une qui oblige les Canadiens à donner leur NAS à leurs institutions financières. Du jour au lendemain, il n'a même plus été possible d'ouvrir un compte bancaire sans donner son NAS. La nouvelle politique a été conçue pour faciliter la communication de renseignements sur les revenus d'intérêts à Revenu Canada; c'est peut-être admissible, mais malheureusement, on n'a à peu près rien fait pour informer le public à l'avance de la raison d'être de cette nouvelle utilisation du NAS.

Le gouvernement avait pourtant promis de consulter le Commissaire à la protection de la vie privée avant de prendre des initiatives dans ce domaine... Il n'en a rien fait avant de présenter son projet de loi. Pour le gouvernement, améliorer l'efficacité de la collecte des impôts justifie une nouvelle utilisation du NAS, sans égard, semble-t-il, au danger qu'elle représente pour la vie privée.

Deux pas en avant

Dans le rapport de l'année dernière, nous avons félicité le gouvernement pour avoir respecté deux de ses engagements, d'abord en adoptant une nouvelle politique régissant son utilisation du numéro d'assurance sociale (NAS), puis en établissant un nouveau système de contrôle du couplage et de l'interconnexion des données. Malheureusement, la rapidité d'exécution du gouvernement est loin d'être à l'égal de l'enthousiasme du Commissaire à la protection de la vie privée. En effet, bien que les politiques sur le NAS et sur le couplage des données aient été annoncées auparavant, elles n'ont été approuvées qu'en avril 1989, après la fin de l'année qui nous intéresse.

Et pourtant, dans ce cas-ci, il faut bien admettre que mieux vaut tard que jamais. Même avec un an de retard, ce sont deux grands pas en avant. (Les mécanismes de réglementation du couplage des données sont décrits de façon détaillée dans le rapport de l'année dernière.)

Il vaut la peine de revenir sur les restrictions que le gouvernement s'est imposées dans son utilisation du NAS, car c'est le plus important des grands engagements qu'il a respectés. Le président du Conseil du Trésor l'a fort bien dit :

« Bon nombre de Canadiens se sentent menacés par l'utilisation qu'on fait de leur numéro d'assurance sociale comme moyen d'identification universel. Etant donné l'évolution rapide de l'informatique, ces personnes se préoccupent de plus en plus de ce que le NAS puisse permettre un accès non justifié à des renseignements personnels et menace de ce fait leur vie privée. »

C'est ainsi qu'a été annoncée la première mesure gouvernementale destinée à réglementer sa collecte et son utilisation du NAS. De nombreuses utilisations actuelles seront éliminées d'ici cinq ans et, dorénavant, toutes les nouvelles collectes du NAS proposées pour des raisons administratives, sauf celles qui figurent sur une liste approuvée, devront être autorisées par le Parlement lui-même.

La nouvelle politique défendra les citoyens contre toutes les pressions bureaucratiques naturelles du secteur public et du secteur privé. Pour la première fois, un gouvernement tente de réduire son utilisation de son propre moyen d'identification numérique. Il est plus facile et moins coûteux de reconnaître les œufs d'une omelette (la politique doit coûter 16 millions de dollars, et c'est peut-être une sous-estimation), mais le gouvernement va de l'avant!

Le NAS ne sera plus le principal numéro d'employé du fonctionnaire; il ne sera plus le numéro du service militaire. Les personnes demandant à résider en permanence au Canada n'arriveront plus chez nous avec un NAS, et l'on pourra présenter une demande de citoyenneté sans être obligé d'avoir un NAS. Les pêcheurs commerciaux qui demandent un permis, les contribuables demandant un remboursement de la taxe sur le combustible, les candidats à des bourses et bien d'autres encore seront désormais libérés de la tyrannie du NAS.

Il est paradoxal que le NAS ait pris tant d'importance dans une société comme la nôtre, si férue de liberté. À l'île-du-Prince-Édouard, on donne aux bébés un NAS comme numéro d'enregistrement de naissance, et certains embaument même allés jusqu'à demander le NAS du défunt. Le cycle est complet, de la naissance à la tombe.

Tout ne va pas pour le mieux

Bref, la protection de la vie privée a connu cette année des hauts et des bas à la Cour suprême. Dans l'administration fédérale, c'était la même chose. La façon la plus équitable d'évaluer le rendement du gouvernement, c'est de voir ce qu'il a fait pour respecter les délais qu'il s'est fixés en publiant en 1987 *Les prochaines étapes*, en réponse aux recommandations unanimes du Comité de la Justice et du Solliciteur général. Dans le rapport de l'an dernier, nous avons accueilli ce document si rassurant avec un respect digne de celui qui fut accordé aux Dix Commandements au pied du Mont Sinaï. Nous disions alors que, quand tout cela sera enfin en place, la troisième génération de législation canadienne en matière de protection des renseignements personnels sera « ce qu'il y a de mieux sur le plan international ».

Le gouvernement s'est donné un plan d'action grâce auquel il devait atteindre tous ses objectifs dès la fin de 1988. Il a pris des engagements précis, notamment d'entreprendre immédiatement l'élargissement du mandat de la Loi sur la protection des renseignements personnels aux sociétés d'Etat fédérales et de créer le Répertoire de renseignements personnels (le guide des fichiers gouvernementaux de renseignements personnels) en tant que base de données lisibles à la machine. Les démarches ont commencé, oui, mais après plus d'un an, le gouvernement n'a pas encore respecté ses engagements.

Et ce n'est pas tout. Le gouvernement aurait dû publier au printemps 1988 des directives régissant la consultation avec le Commissaire à la protection de la vie privée sur les questions liées à la protection des données. Les modifications à la Loi, et notamment les assises légales promises des normes de sécurité de l'information, devaient être introduites pour l'automne 1988. Enfin, un programme de sensibilisation du public à la Loi devait être en place pour l'hiver 1988. Aucune de ces dates n'a été respectée; pire encore, on n'avait même pas commencé le 31 mars 1989.

Bien sûr, c'était des dates limites que le gouvernement s'était fixées à lui-même, et il ne faudrait pas le fustiger pour avoir sous-estimé la difficulté de sa tâche, par excès d'enthousiasme. D'ailleurs, il a respecté certains de ses engagements clés, même s'il l'a fait un peu plus tard qu'il l'avait promis. Il semble globalement déterminé à mener sa tâche à bien.

Pourtant, la lenteur et l'erreur sont bien décevantes.

Les 12 prochains mois nous montreront si *Les prochaines étapes* seront plus qu'une métaphore largement vide de sens, et si la démarche qu'elles ont promise ne sera qu'un exercice de pure forme. Dans le labyrinthe de la protection des renseignements personnels, le conseiller de la Reine de *La Traversée du miroir*, de Lewis Carroll, serait le guide rêvé :

« Ici, voyez-vous, vous devez courir de toutes vos forces pour rester à la même place. Si vous voulez progresser, vous devrez courir au moins deux fois plus vite. »

La Cour suprême a conclu dans *Stewart c. Sa Majesté la Reine* que c'est le Parlement, et non les tribunaux, qui devrait décider quelle protection accorder aux renseignements confidentiels. Le Parlement doit répondre à cet appel à l'action en protégeant l'intégrité de la *Loi sur la protection des renseignements personnels*.

En effet, lorsqu'il a adopté la Loi, le Parlement s'est explicitement engagé envers les Canadiens à respecter la confidentialité des renseignements personnels que le gouvernement détenait à leur égard. Cet engagement, c'est la pierre angulaire de toute la législation sur la protection de la vie privée. S'il est possible de s'approprier des renseignements confidentiels sans avoir à craindre des sanctions parce « qu'on ne peut pas être propriétaire de la confidentialité » la promesse que le Parlement a faite dans la *Loi sur la protection des renseignements personnels* a manifestement perdu une grande partie de sa valeur.

Pouvoir « être propriétaire » de la confidentialité pourrait être bien important que de posséder des objets matériels, car ceux-ci peuvent être remplacés, tandis que la confidentialité perdue ne peut être retrouvée. Ce n'est rien de moins qu'une perte de contrôle qui porte un dur coup à la dignité humaine.

Il reste bien sûr l'abus de confiance, et c'est en vertu de cette accusation qu'on a pu condamner l'employé de Revenu Canada qui avait volé les dossiers de l'impôt sur le revenu de quelque 16 millions de citoyens dans un bureau de Toronto de Revenu Canada. Toutefois, cette accusation ne tiendrait pas dans les cas où des renseignements personnels et confidentiels seraient pris par quelqu'un qui n'est pas fonctionnaire, ou obtenus frauduleusement d'un fonctionnaire ou d'un élu.

Peu de temps après la publication de la décision rendue dans *Stewart c. Sa Majesté la Reine*, le Commissaire a fait état de son inquiétude au ministre de la Justice d'alors, l'honorable Ray Hnatyshyn. Selon le Ministre, le *Code criminel* continuera de dissuader les fonctionnaires de communiquer illégalement des renseignements. M. Hnatyshyn a répété que le gouvernement s'était engagé à modifier la *Loi sur la protection des renseignements personnels* pour créer l'assise juridique des normes de sécurité qui figurent actuellement dans la Politique du gouvernement du Canada sur la sécurité. Le Ministre a souligné les modifications apportées en 1985 aux articles 301.2 et 387(1.1) du *Code criminel*, dans lesquels ont été définies les infractions portant atteinte à l'intégrité des systèmes et des services informatiques, qui protègent les données informatisées, y compris les renseignements personnels.

Pourtant, il reste toujours une brèche que le Parlement devrait combler, parce que le gouvernement conserve d'énormes quantités de renseignements sur support papier et qu'il est impossible d'écarter toute possibilité que des personnes de l'extérieur percent l'écran de sécurité conçu pour les protéger.

La Cour semblait songer surtout, sinon exclusivement, aux risques de préjudice commercial, mais il est certain que de terribles tragédies personnelles risquaient de résulter d'une communication non autorisée des dossiers d'enquête de la Gendarmerie royale du Canada, des rapports de surveillance du Service canadien du renseignement de sécurité et des dossiers médicaux de Santé et Bien-être social Canada — et ce ne sont là que des organismes gouvernementaux. Pourtant, la Cour semble avoir déclaré qu'il est possible de mémoriser, de copier — voire, par implication, de photographier — des documents sans être passible de sanctions pénales, tant qu'on ne s'approprie pas les documents eux-mêmes.

L'affaire *Stewart c. Sa Majesté la Reine* n'a pas reçu toute l'attention du public qu'elle méritait. S'il s'était agi de renseignements à caractère délicat sur la santé — ou de dossiers financiers — plutôt que d'une liste de noms de personnes impliquées dans un vulgaire conflit de travail, il y aurait eu une véritable tempête de protestations, et à juste titre.

La *Loi sur la protection des renseignements personnels* ne prévoit pas de sanctions. Jusqu'à ce que la décision de la Cour suprême ait été rendue publique, une condamnation pour vol, en vertu du paragraphe 298(1) du *Code criminel*, ou pour fraude, en vertu du paragraphe 328(1) dudit Code, semblait suffisante comme moyen de dissuasion. Par conséquent, on n'a pas jugé utile que la *Loi sur la protection des renseignements personnels* prévienne elle-même des sanctions. Avec le jugement *Stewart*, la protection du Code criminel s'est envolée.

La condamnation prononcée par la Cour d'appel de l'Ontario a été renversée à l'unanimité par la Cour suprême. Le juge Antonio Lamer a rédigé la décision de la Cour en concluant que «... les renseignements confidentiels ne sont pas d'une nature telle qu'ils peuvent être détournés parce que, si l'on s'approprie des renseignements confidentiels sans s'emparer d'un objet matériel, par exemple en mémorisant ou en copiant des renseignements... le prétendu propriétaire ne se voit privé ni de l'usage, ni de la possession de ces renseignements ». Plus loin, le juge a souligné que «... on ne peut être privé de la confidentialité parce qu'on ne peut pas en être propriétaire ».

Avec tout le respect que nous devons à la Cour, pour imiter la formule rituelle des avocats, force nous est de dire que ces observations ont des implications alarmantes pour la société de l'information en général et pour la *Loi sur la protection des renseignements personnels* en particulier. Si la Loi promet quelque chose, c'est bien de protéger la confidentialité des renseignements personnels recueillis par les institutions gouvernementales. La subtile distinction juridique sur la possibilité ou l'impossibilité pour la confidentialité d'être un bien n'a tout simplement aucune pertinence dans un contexte où il faut préserver la confidentialité de renseignements de nature délicate.

Si cette interprétation de profane de la décision de la Cour est valide, nous devons conclure que la Cour n'a pas accordé suffisamment d'importance au grave préjudice qui pourrait résulter d'un accès non autorisé aux masses énormes de renseignements personnels délicats que détiennent le gouvernement et le secteur privé.

Dans notre domaine, l'évaluation des résultats d'un an de travail est entièrement fonction des normes utilisées. Essayer de résumer la situation en quelques formules accrocheuses, c'est risquer de verser dans la fausse représentation, car la question est désormais bien trop complexe.

Même la Cour suprême du Canada a contribué à nuancer les résultats, en déclarant dans *Sa Majesté la Reine c. Brandon Roy Dymnt* que « la notion de vie privée est essentielle au bien-être de la personne » et que « l'interdiction qui est faite au gouvernement de s'immiscer de trop près à la vie des citoyens touche à l'essence même de l'État démocratique ». Le message ne saurait être plus clair et la source plus digne de foi.

Dans ce jugement, la Cour a renforcé l'opinion qu'elle avait déjà formulée en déclarant que la protection des « particuliers » contre les intrusions injustifiées... dans leur vie privée » est établie par l'article 8 de la Charte canadienne des droits et libertés (« Chacun a droit à la protection contre les fouilles, les perquisitions ou les saisies abusives »). Le jugement rendu dans l'affaire Dymnt, rédigé par le juge G.V. La Forest, a aussi posé un principe fondamental, le suivant : « ...si le droit à la vie privée de l'individu doit être protégé, nous ne pouvons pas nous permettre de ne faire valoir ce droit qu'après qu'il a été violé... Il faut empêcher les atteintes au droit à la vie privée et, lorsque d'autres exigences de la société l'emportent sur ce droit, il doit y avoir des règles claires qui énoncent les conditions dans lesquelles il peut être enfreint. »

La Loi sur la protection des renseignements personnels est précisément un ensemble de règles comme celles-là. Jusqu'à présent, la Cour suprême a rendu deux décisions qui lui ont donné d'excellentes assises constitutionnelles, en établissant explicitement la protection de la vie privée en vertu de l'article 8 de la Charte.

Le Parlement peut tirer fierté d'être allé plus loin que la Charte et la Cour suprême en établissant dans la Loi sur la protection des renseignements personnels les règles régissant les utilisations gouvernementales des renseignements personnels obtenus des citoyens. En ces jours où les différends sont nombreux, le Parlement n'a pas toujours cette longueur d'avance sur les tribunaux.

Et pourtant, le front juridique n'est pas toujours une source de joie sans mélange pour les protecteurs de la vie privée. Ainsi, la décision de la Cour suprême dans *Stewart c. Sa Majesté la Reine* semble marquer un recul. Dans cette affaire, la Cour a jugé qu'il est impossible de voler des renseignements confidentiels, parce qu'on ne peut les considérer comme un bien au sens du Code criminel.

L'affaire est connue : un syndicat qui tentait de former une unité de négociation dans un hôtel n'avait pu obtenir les noms et les adresses de quelques 600 employés, parce que la direction considérait ces renseignements comme confidentiels. Un consultant embauché par le syndicat s'est procuré la liste par l'entremise d'un gardien de sécurité qu'il avait soudoyé pour copier les noms d'une liste conservée à l'hôtel, sans en sortir l'original et sans le modifier le moins possible. Le consultant a été accusé au pénal d'avoir incité à commettre une fraude, un vol et un méfait en portant atteinte à la propriété privée de l'hôtel et de ses employés.

La Loi sur la protection des renseignements personnels donne aux individus accès à leurs renseignements personnels détenus par le gouvernement fédéral; protège la vie privée des individus en restreignant le nombre des personnes qui peuvent consulter les renseignements; et donne aux individus un certain contrôle sur la collecte et l'usage des renseignements par le gouvernement.

La Loi énonce les principes des pratiques équitables en matière d'information qui exigent que le gouvernement :

- ne collecte que les renseignements dont il a besoin pour exécuter ses programmes;

- recueille les renseignements directement auprès de l'individu concerné, dans la mesure du possible;

- informe l'individu des fins auxquelles ils sont destinés;

- conserve les renseignements suffisamment longtemps pour en assurer l'accès aux individus; et

- veille « dans la mesure du possible » à ce que les renseignements personnels soient exacts et complets.

Toute personne présente au Canada peut déposer une plainte auprès du Commissaire à la protection de la vie privée si :

- elle s'est vu refuser une partie quelconque des renseignements;
- le droit de demander la correction de certains des renseignements contenus dans le fichier ou de les annuler leur est refusé;
- le ministère prend plus des 30 jours initiaux ou des 60 jours maximums pour fournir les renseignements;

- la description du contenu des fichiers de renseignements donnée dans le Répertoire des renseignements personnels est incorrecte à un quelconque égard;
- la liste donnée dans le Répertoire pour chaque ministère ne décrit pas tous les usages qui sont faits des renseignements personnels; une institution recueille, conserve, utilise ou élimine des renseignements personnels d'une manière qui contrevient à la Loi sur la protection des renseignements personnels.

Les enquêteurs du Commissaire à la protection de la vie privée examinent tous les fichiers (y compris ceux considérés inconsultables), à l'exception des renseignements confidentiels du Conseil privé de la Reine, pour s'assurer que les institutions fédérales se conforment à la Loi. La Loi confère également au Commissaire à la protection de la vie privée le pouvoir de vérifier la façon dont les institutions fédérales recueillent, utilisent et éliminent les renseignements personnels, sans devoir attendre qu'une plainte soit déposée.

Table des matières

Mandat	1
Des hauts et des bas	2
Mais qui décide?	11
La protection de la vie privée dans le contexte du SIDA	15
À l'aube de l'ère biotechnologique	18
Sécurité informatique	20
Les dossiers du SCRS	22
Qu'est-ce qu'il y a avec le chèque?	24
Direction générale des plaintes	26
Dossiers	28
Demandes de renseignements	37
Direction générale de l'observation	43
Société canadienne des postes	47
Commission d'appel des pensions	49
Conseil des sciences du Canada	50
Ministère des Finances	51
Secrétariat du Solliciteur général	52
Emploi et Immigration Canada (EIC)	53
Aviser le Commissaire	57
Faites passer	60
Gestion intégrée	61
Annexe I	63
Annexe II	64

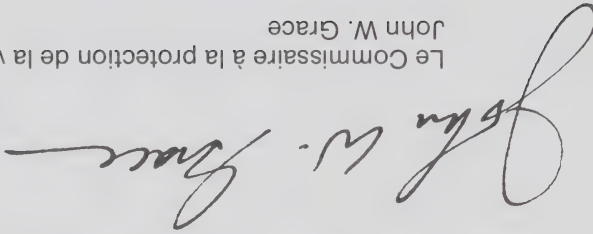
L'honorable John A. Fraser, c.p., c.r., député
Président
Chambre des communes
Ottawa

le 30 juin 1989

Monsieur Fraser,

J'ai l'honneur de soumettre mon rapport annuel au Parlement. Ce rapport couvre la période allant du 1er avril 1988 au 31 mars 1989.

Veuillez agréer l'expression de mes sentiments respectueux.



Le Commissaire à la protection de la vie privée,
John W. Grace

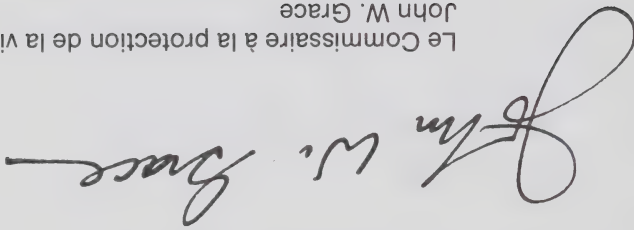
L'honorable Guy Charbonneau
Président
Sénat
Ottawa

le 30 juin 1989

Monsieur Charbonneau,

J'ai l'honneur de soumettre mon rapport annuel au Parlement. Ce rapport couvre la période allant du 1er avril 1988 au 31 mars 1989.

Veuillez agréer l'expression de mes sentiments respectueux.

A handwritten signature in dark ink, reading "John W. Grace". The signature is written in a cursive style with a large, looping initial "J".

Le Commissaire à la protection de la vie privée,
John W. Grace

“Les seuls renseignements personnels que peut recueillir une institution fédérale sont ceux qui ont un lien direct avec ses programmes ou ses activités”

“Une institution fédérale est tenue de recueillir auprès de l'individu lui-même, chaque fois que possible, les renseignements personnels . . . le concernant”

“ . . . est tenue d'informer l'individu . . . des fins auxquelles ils (les renseignements personnels) sont destinés”.

“ . . . est tenue de veiller, dans la mesure du possible, à ce que les renseignements personnels . . . soient à jour, exacts et complets”.

“À défaut du consentement de l'individu concerné, les renseignements personnels relevant d'une institution fédérale ne peuvent servir à celle-ci : a) qu'aux fins auxquelles ils ont été recueillis ou préparés”

(ou conformément aux exceptions précises énoncées à l'article 8)
La Loi sur la protection des renseignements personnels.

Le Commissaire à la protection de la vie privée du Canada
112, rue Kent,
Ottawa (Ontario)
K1A 1H3

(613) 995-2410
1-800-267-0441

© Ministre des Approvisionnement et Services Canada 1989
N° de cat. IP 30-1 / 1989
ISBN 0-662-56842-7

Rapport annuel du Commissaire à la protection de la vie privée

1988-89



**Commissaire à la
protection de la vie privée**



Rapport annuel 1988-89



For 1989/90 issue see:

CA7

MM

-P65

#90-06898

CAI
PC
- A57

General
Information

Privacy Commissioner Annual Report 1990-1991



**Annual Report
Privacy Commissioner
1990-91**



The Privacy Commissioner of Canada
112 Kent Street
Ottawa, Ontario
K1A 1H3

(613) 995-2410, 1-800-267-0441
Fax (613) 995-1501

© Minister of Supply and Services Canada 1991

Cat. No. IP30-1/1991

ISBN 0-662-58483-X

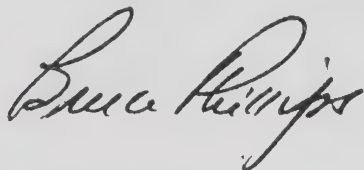
The Honourable Guy Charbonneau
The Speaker
The Senate
Ottawa

June 28, 1991

Dear Mr. Charbonneau:

I have the honour to submit to Parliament my annual report. This report covers the period from April 1, 1990 to March 31, 1991.

Yours sincerely,

A handwritten signature in cursive script, reading "Bruce Phillips". The signature is written in dark ink and is positioned below the "Yours sincerely," text.

Bruce Phillips
Privacy Commissioner

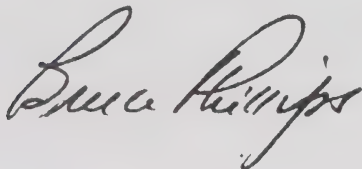
The Honourable John Fraser, P.C., Q.C., M.P.
The Speaker
The House of Commons
Ottawa

June 28, 1991

Dear Mr. Fraser:

I have the honour to submit to Parliament my annual report. This report covers the period from April 1, 1990 to March 31, 1991.

Yours sincerely,

A handwritten signature in cursive script, reading "Bruce Phillips". The signature is written in dark ink and is positioned above the printed name and title.

Bruce Phillips
Privacy Commissioner

Table of Contents

Mandate	1
New conductor, familiar score.....	2
Privacy and the Charter	8
Cellular phones and privacy.....	13
Privacy in the private sector.....	15
Biomedical testing.....	18
Electoral reform—a permanent voters' list.....	22
Privacy and the public interest: a difficult balance	24
Complaints directorate	26
Directorate report.....	26
Tables and charts	30
Cases.....	35
Notifying the Commissioner.....	44
Policy and research	47
Data matching	47
Technology marches on	52
Consulting the Commissioner	54
Inquiries	55
Compliance directorate	57
Corporate management.....	61
Organization chart.....	63

Mandate

The *Privacy Act* provides individuals with access to their personal information held by the federal government; it protects individuals' privacy by limiting those who may see the information; and it gives individuals some control over the government's collection and use of the information.

The Act sets out the principles of fair information practices, requiring government to :

- collect only the information needed to operate its programs;
- collect the information directly from the individual concerned, whenever possible;
- tell the individual how it will be used;
- keep the information long enough to ensure an individual access; and
- "take all reasonable steps" to ensure its accuracy and completeness.

Individuals in Canada may complain to the Privacy Commissioner if:

- they are denied any part of the information;
- they are denied their request to correct some of the information on the file— or their right to annotate it;
- the department takes longer than the initial 30 days or maximum 60 days to provide the information;
- the **Info Source** description of the contents of the information bank is deficient in some way;
- the department's listing in the Source does not describe all the uses it makes of personal information;

- an institution is collecting, keeping, using or disposing of personal information in a way which contravenes the *Privacy Act*.

The Privacy Commissioner's investigators examine any file (including those in closed banks) except confidences of the Queen's Privy Council to ensure that government institutions are complying with the Act.

The Act also gives the Privacy Commissioner the power to audit the way government institutions are collecting, using and disposing of personal information.

New Conductor, Familiar Score

This is the first annual report to Parliament in eight years to be submitted by anyone other than John Grace who, until June, 1990, was the sole person to have served as Privacy Commissioner of Canada since the office was established as a function separate from the Canadian Human Rights Commission in 1983.

Mr. Grace completed his term of office in July of 1990 and assumed new duties as Canada's Information Commissioner. He departed this office with a high reputation in several respects: first, as an ombudsman with an outstanding gift for resolving privacy problems and complaints; second, as an energetic and eloquent spokesman for the cause of protection of personal privacy, and third, as the respected leader of a small but highly-motivated staff of skilled investigators and auditors who reflected his abiding concern for this vital but embattled area of human rights.

He also was ever alert to the new challenges to privacy protection which continue to arise with almost bewildering rapidity and number in a constantly-changing commercial and technological environment.

Thus Mr. Grace has bequeathed to his successor the advantage of a smoothly-functioning organization. Many of the issues touched upon in this report were initiated prior to Mr. Grace's departure.

During the interval between the departure of the former commissioner and the confirmation of a new one, a period of some ten months, the duties of acting commissioner were performed by the executive director, Alan Leadbeater. He served with distinction in the difficult dual role of both administrative head and ombudsman.

The new commissioner, coming into office almost on the eve of this report, is acting in some senses as a surrogate spokesperson for two predecessors, although he was, as assistant commissioner, the beneficiary of their experienced counsel and guidance. In fact, the ten months expended as assistant commissioner proved to be an invaluable introductory exposure to a field which is both complex and becoming more so. If the reader detects any diffidence in the tone of the observations, be assured it is attributable to the realization that the author still has much to learn.

It may be small comfort to this neophyte that he is not alone. In fact, the privacy guard also changed in Ontario and Quebec during the year. Paul-André Comeau was appointed Quebec's new Access and Privacy Commissioner and Thomas Wright was named Information and Privacy Commissioner of Ontario. One thing should not change—the cordial and mutually supportive relationship among these offices.

This report, in attempting to give a reading on the state of privacy protection in the nation, will share with its predecessors something of the quality of a "good news-bad news" story. It is the nature of the issue that there will be no final victories. Personal privacy is a problem intimately bound up with the relationship of the individual to society, and so long as society continues to evolve and change, so too will the problems affecting privacy.

There is no more fragile, yet important, right in today's complex society than the right to a reasonable expectation of privacy. It is not a right, which some cynics suggest, that only serves those with something to hide. Without a meaningful measure of privacy our fundamental freedoms of expression, belief and association risk becoming meaningless.

Justice Brandeis, in his famous 1898 definition of privacy as "the right to be let alone", could not have contemplated a world of ingenious machines with unlimited capacity for collecting, collating and transmitting information across global networks. Nor could he have foreseen a science capable of plumbing the deepest secrets of human heredity.

The right to be left entirely alone, if it ever existed, could now be exercised, if at all, only, in the farthest corner of the most remote reaches of our arctic. Even then, one suspects, the putative recluse would sooner or later see some indomitable servant of a government department looming over the frozen horizon bearing the all-important form which, when properly filled out, would confer that indisputable certification of human existence, a Social Insurance Number.

But if absolute privacy in modern society is neither attainable, practical nor even particularly desirable, the struggle must continue to preserve the individual's right to decide the degree to which personal privacy is to be sacrificed on behalf of other competing rights and claims.

So the notion of an annual fever-chart, while it provides a convenient method of keeping score, is to a certain extent misleading unless it is clearly understood that, where privacy is concerned, the patient will always be in danger since it is under assault from new afflictions as rapidly as remedies for older ones are found.

One is struck by this phenomenon in reading past annual reports. Many of the issues which dominate privacy discussions today were barely in the privacy vocabulary eight short years ago. For example there is drug testing, AIDS testing, and implications of genetic research, interception of cellular telephone communications, to name but a few, and some of which will be referred to later in this report. Doubtless this will continue to be the experience in future, since there is no reason to believe there will be any relaxation in the onward march of science and technology. The best one can do is to stand firmly on the privacy ramparts, trying to dam the breaches as they occur, and confident of nothing except that it will be a never-ending struggle.

So how did the struggle proceed in the year just past?

Certainly there is no reason on the available evidence to suppose there has been any abatement in the technological onslaught against personal privacy. Computers continue to proliferate (80,000 in the possession of the federal government alone, at last estimate), the tide of junk mail continues to mount, the commercial trafficking in personal information continues to increase (a \$3 billion annual business in the U.S., and, presumably, on the usual proportion, at least \$300 million in Canada).

But, on the proposition that an aroused and informed public is the best bulwark of privacy rights, there are very positive signs of real and lasting gains.

In the marketplace

Past reports have referred to the growing awareness of invasive marketing practices in the private sector. In 1990, the issue received the final accolade of media stardom—a TIME Magazine cover story. And although some of the participants might have wished otherwise, further proof of the rising profile of privacy issues emerged in the political arena in two provinces where ministers found themselves in difficulties over disclosures which, in two cases at least, led to a resignation. Whatever else one might think or say about them, these events underline that privacy rights cannot always be ignored with impunity. And, if the marketplace in recent years has generated some of the major threats to privacy, the marketplace acting in self-interest in the end may also prove to be at least partly a self-correcting mechanism.

Presumably in response to growing consumer concern, the private sector is showing (at long last, some might say) encouraging signs of action. During the past year, the Canadian Bankers Association, Bell Canada and the Canadian Direct Marketing Association have all produced codes offering significant improvements in the protection for privacy and confidentiality of information concerning their clients. These developments are discussed in more detail later in the report, but here it is worth noting that they offer some hope yet for the path of voluntary action.

The issue now is not whether the private sector can continue without privacy codes, but how long it will be before compulsion in one form or another enters the equation. Thanks to developments in Europe, North American business may soon lose its ability to engage in data transfers with European business unless it has privacy codes in place. This development lends added urgency to the Commissioner's recommendation to Parliament last year that the *Privacy Act* be amended to require all federally-regulated private sector firms to implement privacy codes based on internationally-accepted guidelines and principles.

Even assuming such voluntary codes become a feature of the Canadian marketplace, there remains a question about their effectiveness. Highly-respected authorities believe some form of oversight is necessary before business becomes truly accountable to the public for protecting privacy.

Dr. David Flaherty, the leading Canadian academic in the field of privacy research, argues that a federal audit power is required to ensure private sector compliance with its own voluntary codes. His is a view which must be respected, yet the Commissioner continues to hope (as did his predecessor) that such a degree of intervention (with the massive resources it implies) may be forestalled by the private sector demonstrating some good privacy citizenship.

Certainly there remains a long way to go. Citing one small example, some chartered banks in their credit card applications still include in the fine print virtual absolute waivers of the privacy rights of customers. These waivers confer upon the banks the right to re-use, in any way they see fit, any or all of the information provided, such as salary, employment history, personal assets and in one case, the Social Insurance Number. A few sharp-eyed consumers have noted these waivers and drawn them to the attention of this office but most, we suspect, did not notice. Such fine-print caveats do not meet any reasonable definition of "informed consent". Neither do they reflect the spirit of enhanced respect for privacy to which the chartered banks' own association now lays claim.

On the positive side, the Canadian Direct Marketing Association is commended for providing a process by which consumers may have their names removed from the mailing lists of their members. Since the association covers more than 80 per cent of the firms engaged in direct marketing, this is a forward step.

Still, such modest improvements are in no way keeping pace with the exploding volume of information exchange made possible by the computer. Thus a minimum step to imposing some standards on the trade in personal information should be the introduction of a legislated requirement that all business under federal jurisdiction implement approved privacy codes. The Commissioner considers this urgent.

Also needed is for Parliament to restore privacy to telephone communications in Canada, now eroding with the spread of cellular telephones. Cellular communications can and are being intercepted by easily available monitoring equipment. There seems no reason why the absence of conventional wires should deprive customers of the right and expectation of privacy. Sale or possession of monitoring equipment should be limited to authorized organizations for use only in conformity with laws governing surveillance activities.

Appraising the manager

Readers of last year's report may recall the Commissioner's cool reception of a proposed hotline for anonymous tips from public servants about government fraud, waste and mismanagement. Happily the idea was dropped.

But many of the same privacy problems are inherent in a new management tool departments are taking up with enthusiasm—"reverse" or "upward" appraisals. As the terms imply, the process allows employees to evaluate their managers' performance anonymously. Although it has been used by large private sector corporations, this is a novelty for government agencies which, as part of public service reform, now design their own appraisal systems.

The process requires employees to complete a questionnaire, rating managers on their management skills and personal traits. The completed forms then are analyzed, sometimes by a private consultant, and summarized. Managers receive a copy but do not see individual employees' ratings or comments.

There are several privacy problems in the process—first is promising employees confidentiality to prevent reprisals. The *Privacy Act* gives individuals the right to see what others say or write about them. And so promising confidentiality to employees who complete the appraisals is misleading and hollow.

In contrast, it is firmly established public service practice for employees to review, comment on and even (if they wish) appeal managers' appraisals of their performance.

Second, the notion that privacy rights can be sidestepped by contracting out the process is dangerous and unsupportable. To accept such a view would mean that all government privacy objectives could be foresworn by turning personal information over to private contractors. The implications go well beyond concern that managers would lose their right of access and that the Act would not protect this highly personal information from improper use or disclosure. However, once hired, contractors are agents of the government and it retains "control" of the information, wherever it happens to be stored.

Few would argue with government's aim to improve management and accountability. But establishing a process which subverts its own legislation is hardly the proper weapon.

A year at the office

As it has in almost every year since the office was established, the number of complaints, investigations, and audits has increased. Although the details are compiled in separate chapters elsewhere in this report, the office is now working at full stretch and, general restraint notwithstanding, Honorable Members and Senators must understand that the obligations they have laid on the office under the *Privacy Act* can not be discharged at their present level of efficiency by the existing modest staff of 34 persons. Investigations now number more than 1,200 a year, exceeding 100 per investigator. Any significant increase in this workload, which experience suggests is inevitable, simply cannot occur without sacrificing existing standards of service.

The compliance branch also had a busy year, but it is worth noting that after eight years of operation, it has managed audits in only about one-fifth of the 150 federal departments and agencies covered by the *Privacy Act*. Clearly, if the reach of the Act is ever extended to include audit responsibilities in the private sector, the existing compliance branch of nine persons will be unequal to the task.

On the research side, the major effort of the office during the previous year was a study of the privacy implications of drug testing. The study found that mandatory random drug-testing in the workplace was unjustified, and in some circumstances, probably illegal. The office notes with approval that the Department of Transport has modified to some extent its drug-testing plans, but disapproves of the Department of National Defence and at least one chartered bank going forward with drug-testing programs which constitute unwarranted breaches of personal privacy. This issue is discussed in greater detail in a separate chapter.

Now in the final stages of preparation is a study on the implications of progress in genetic research and testing, a subject which holds the promise of even greater privacy problems than drug-testing. The report is expected to be published in late summer of 1991.

Privacy and the Charter

It is both fascinating and gratifying for a Privacy Commissioner to watch the Supreme Court of Canada fashion a prominent place for the right to privacy within the *Canadian Charter of Rights and Freedoms*. It is fascinating for the ups and downs of the saga — and gratifying for the overall growing strength of the right to privacy.

Two previous annual reports followed this unfolding study. There is more to tell this year.

On September 11, 1983, police seized 278 pounds of marijuana from a vehicle and charged a number of individuals with conspiracy to import an illegal substance. The Crown's case was based on 136 phone calls intercepted during an intensive investigation in widely separated areas of British Columbia.

The police believed that the alleged conspirators used public pay telephones to conduct their affairs and so they installed listening devices on 20 public pay phones. Tape recorders were attached to pay phones on some 20 occasions and left on automatic record overnight, intercepting and recording conversations of suspects and others. While the police obtained judicial authorizations for these wiretaps, none of the authorizations specifically allowed the bugging of pay phones. Rather, the authorizations employed a "basket clause" giving police the authority to intercept communications at certain addresses and "...elsewhere in the Province of British Columbia resorted to by (the suspects)...".

The trial judge ruled that, in these circumstances, the judicial authorizations were invalid. In his view, the automatic monitoring of public pay phones when such monitoring is not specifically authorized by a judge, permits a dragnet type of investigation not contemplated by the *Criminal Code*. He ruled the intercepted communication inadmissible and directed the jury to acquit the accused.

The B.C. Court of Appeal saw it differently, reversed the trial judge's decision and ordered a new trial. The Court of Appeal concluded that it was not necessary for the authorization to make specific reference to pay phones as long as any monitoring of pay phones was not indiscriminate. The Court of Appeal found that an intercepted communication itself could (by containing a suspect's voice) provide evidence that the monitoring was not indiscriminate.

The Supreme Court of Canada resolved the matter in a 4-2 decision, *Thompson, et al v. The Queen*, issued October 18, 1990. The Supreme Court conclusion is most interesting, if puzzling.

Writing for the majority, Justice Sopinka concluded that the "basket clause" authorization was lawful even though no mention was made of public pay phones nor were any limiting conditions imposed to protect the public. However, he wondered whether the interceptions which took place in this case pursuant to the valid authorizations were "reasonable" under section 8 of the *Charter*.

He concluded that in at least four instances, taps were placed on public pay phones solely because they were near where a suspect was staying and that this was insufficient evidence to act upon, "... (it) amounts to little more than indiscriminate monitoring based on a hunch" (p. 26). Furthermore, since this jeopardized the right to privacy of innocent third parties (hundreds of private conversations may have been intercepted when not one target was involved), Justice Sopinka concluded that it infringed upon section 8 of the *Charter*.

Now the puzzling part. Justice Sopinka reasoned that it would not bring the administration of justice into disrepute to admit the evidence obtained from wiretapped public pay phones. Consequently, the appeal was dismissed and a new trial ordered.

What comfort does this give us? Strong admonitions are made against relying on the "basket clauses" in wiretap authorizations. Judges and the police are strongly encouraged by the Court to minimize the intrusions upon the privacy of innocent third parties when seeking or granting wiretap authorizations and when intercepting communications. Yet, the law enforcement community is essentially told that if it fails to live up to these standards, no matter — their cases will not be jeopardized.

The dissenting opinions of Justice La Forest and Justice Wilson point out the shortcomings in the thinking of the majority. Both said that since the tapping of public pay phones give rise, *per se*, to massive violations of privacy, judicial authorizations for such activity must be expressly made and not granted by implication under the "resort to" basket clause. By not taking this view, the Supreme Court has left it to Parliament to ensure that *Charter* infringements are not perpetrated by the police. How completely the respective roles of the *Charter* and Parliament have been turned. Justice La Forest puts it eloquently:

"It will be obvious that the Act (*Criminal Code*) and the *Charter* place a heavy burden on the courts to ensure the privacy of Canadians. Electronic surveillance is indiscriminately acquisitive; its reach extends to the conversations of the innocent and the guilty alike. The indiscriminate acquisitiveness of electronic surveillance invites the courts to redouble their vigilance and to be especially sensitive of the potential of certain practices to undermine the expectation of Canadians that their private communications are inviolable. This legitimate and reasonable expectation of privacy will not long survive if the courts give their *imprimatur* to practices that allow the police to intercept private communications solely on the basis of their own reasonable belief that valuable evidence stands to be gained thereby. In my view, 'resorted to' clauses can easily result in the application of this low threshold and constitute the 'fishing expeditions of considerable latitude' decried by this

court in *Hunter v. Southam, supra*, at p. 167. It is sad to reflect that, even with the assistance of the *Charter*, the courts have failed to take the steps necessary to avoid this danger and that if Canadians are to receive adequate protection against the insidious threat to individual privacy posed by electronic surveillance, they must turn to Parliament to provide additional safeguards. There is biting irony in this. The *Charter* was designed to protect us from possible inroads on individual rights by Parliament". (pp. 13-14)

And so, a Privacy Commissioner, at best, has mixed emotions about the *Thompson* decision. We must applaud the Court's new insistence that, when police intercept private communications, the privacy rights of innocent third parties must be protected. There is a strong message to judges and the police to be especially vigilant when wiretaps are installed at places frequented by the public. Although the Court does not make it a mandatory requirement, it suggests that visual surveillance accompany the wiretap to ensure that only a suspect's conversations are intercepted. Canadians should be comforted by the Supreme Court's consciousness of privacy threats to innocent parties when police engage in wiretapping. Nevertheless, the Court also makes it clear that if Canadians are to be adequately protected against these abuses, Parliament must act to strengthen the wiretap provisions of the *Criminal Code*.

Therefore, the Privacy Commissioner urges the government to propose, and Parliament to enact, measures necessary to ensure adequate control of wiretapping practices.

This year's Supreme Court privacy story, however, does not end with a whimper. Its decision in the case of *Santiago Wong v. The Queen* (November 22, 1990) is a bang.

The *Wong* case resulted from a Toronto police gambling investigation conducted during the summer of 1984. The security staff of a major downtown hotel told police they suspected that hotel premises were being used for illegal gambling. There was evidence of gambling in a recently vacated hotel room and the police learned that the person who had reserved the room, Mr. Wong, had also reserved it for later the same month.

The police installed a video camera in the room with the permission of the hotel management but without judicial authorization or warrant. Activities in the room were monitored on five separate occasions and resulted in charges being laid against Mr. Wong and ten others for keeping a common gaming house.

The trial judge found that the video surveillance was an infringement of section 8 of the *Charter* and dismissed all charges. The Ontario Court of Appeal, however, noted that invitations had been widely circulated within the Chinese community and that strangers who came to the hotel room were welcomed. In these circumstances, the court found that the accused had no reasonable expectation of privacy and that, as a result, section 8 of the *Charter* did not apply. A new trial was ordered.

On appeal the Supreme Court, in a 6-1 decision, took a different view. It concluded that without judicial authorization, such video surveillance was an infringement of the section 8 protection against unreasonable search and seizure. This decision is especially remarkable because it extends the privacy right to a right to freedom from indiscriminate video surveillance by agents of the state. The Court concluded that this privacy right must be protected by an independent judiciary and that police cannot be left to decide when video surveillance may be employed.

In his majority judgment, Justice La Forest is clear that all forms of electronic surveillance by agencies of the state, not judicially authorized, violate section 8 of the *Charter*.

"...the broad and general right to be secure from unreasonable search and seizure guaranteed by s. 8 is meant to keep pace with technological development, and, accordingly, to ensure that we are ever protected against unauthorized intrusions upon our privacy by agents of the state, whatever technical forms the means of invasion may take." (p. 6)

As a result of *Wong*, it is no longer appropriate for a court to inquire into whether a person who is the subject of unauthorized surveillance has "courted the risk".

In Justice La Forest's words:

"...privacy would be inadequately protected if an assessment of the reasonableness of a given expectation of privacy were made to rest on a consideration whether the person concerned had courted the risk of electronic surveillance. In view of the advanced state of surveillance technology, this would be to adopt a meaningless standard, for, in the final analysis, the technical resources which agents of the state have at their disposal ensure that we now run the risk of having our words recorded virtually every time we speak to another human being." (p. 7)

Thus, despite the fact that the accused had widely issued invitations to his hotel room and opened the door to strangers, he did not lose his right to a reasonable expectation of privacy. The Court made it clear that while we might impose warrantless video surveillance on those who engage in illegal activities in their hotel rooms, society would object to imposing that risk on anyone who rents rooms. In order to avoid the latter, the Court considered that it must prohibit the former.

Unlike wiretapping, there is currently no available procedure for police to obtain a judicial authorization for video surveillance. The Court was fully aware of the handicap its decision imposed upon the police, but felt that only Parliament should decide the circumstances in which the police could invade privacy by means of video surveillance.

In Justice La Forest's words:

"On my view of the matter the courts would be forgetting their role as guardians of our fundamental liberties if they were to usurp the role of Parliament and purport to give their sanction to video surveillance by adopting for that purpose a code of procedure dealing with an altogether different surveillance technology. It is for Parliament, and Parliament alone, to set out the conditions under which law enforcement agencies may employ video surveillance technology in their fight against crime. Moreover, the same holds true for any other technology which the progress of science places at the disposal of the state in the years to come." (p. 22)

No doubt the government will introduce legislation to provide for the judicial authorization of video surveillance by the police. That would be the responsible course since no one questions the need for video surveillance in law enforcement. However, as with wiretapping, the Privacy Commissioner urges Parliament to ensure that any process for obtaining judicial authorization for video surveillance protects the privacy of innocent parties.

Cellular Phones and Privacy

In the past year Canadians have become aware—some painfully so—that cellular telephone calls can be intercepted.

One British Columbia cabinet minister resigned after a newspaper printed extracts from calls he made on his car phone. Some provincial delegations at the Meech Lake Conference suspected that their cellular communications had been intercepted. And a provincial power corporation was embarrassed when someone intercepted and published an employee's comments about third parties during a cellular phone conversation.

Faced with this troubling new threat to privacy, the Commissioner has tackled two questions:

- Does the *Privacy Act* protect cellular phone calls?
- And do federal government institutions, including its law enforcement agencies, only intercept cellular communications in compliance with the law?

The Supreme Court decisions (discussed above) make it clear that, without proper judicial authorization, agencies of the state may not subject individuals to any form of electronic surveillance. To do so would be "improper search and seizure". It would sacrifice our right to a reasonable expectation of privacy, thus infringing section 8 of the *Charter of Rights and Freedoms*.

The state may no longer assume that individuals have waived their right to privacy just because they "court the risk" of surveillance by, for example, using a communications technology known to be vulnerable to interception. According to the Supreme Court, that assumption would incur a greater risk—that electronic surveillance without a proper warrant would so dilute our privacy as to be inconsistent with a free and open society.

That conclusion has direct implications for the *Privacy Act*. The Act controls the collection of personal information by federal institutions. Principal among these controls is one which prohibits collecting personal information "...unless it relates directly to an operating program or activity of the institution" (section 4).

This provision is open to interpretation in specific cases. But it cannot be read to sanction a collection of personal information which would otherwise be unlawful. Collecting personal information in a way which violates the Charter would also breach the *Privacy Act*.

Since the *Privacy Act* is implicated when federal investigative bodies intercept cellular calls, the Privacy Commissioner wants to satisfy himself that any federal interceptions comply with the Act. However, the emphasis is on fact-finding. There is no reason to believe that federal authorities are unlawfully invading the privacy of Canadians' cellular phone calls.

The commissioner is making inquiries and anticipates reporting the results in next year's annual report.

More troubling is the absence of any legal control over private citizens intercepting cellular phone calls. As one commentator puts it:

“While the average cellular telephone user may be prepared to contend with occasionally finding another conversation sharing his line, he may be concerned to discover that conversations can be deliberately monitored using something as simple as an old TV set capable of receiving cellular UHF frequency”.(Network Newsletter, Vol. 10, No. 24, July 30, 1990, p.1)

Using the *Charter*, the Supreme Court has cobbled together protections against cellular monitoring by agents of the state, but the *Charter* does not control individuals' behaviour. And it is doubtful whether current *Criminal Code* provisions prohibiting the surreptitious interception of private communications apply to cellular phone calls. After all, a cellular communication is carried on radio waves and so may not be considered “private”.

Some other jurisdictions—California, for example—have passed laws prohibiting both interception of cellular calls and the sale or purchase of cellular eavesdropping devices. An even broader law is before the U.S. Congress covering computer communications and radio communications (H.R.3378 and S.1667). That proposal would make it unlawful to eavesdrop on a car phone conversation or any other private radio communication.

Of course, laws in themselves cannot ensure that cellular conversations remain private. In fact, some argue that such laws could lull cellular phone users into a false sense of security and, hence, be counterproductive. The Commissioner does not agree. It is vital for Parliament to act quickly to protect the privacy of cellular phone users. The mere disappearance of the wires which once carried our communications must not end in the disappearance of our privacy.

Privacy in the Private Sector

In a highly computerized society information knows no boundaries. Yet Canada contents itself with an information policy which distinguishes between the government and the private sector. There is some legal protection against information abuses in the federal (and some provincial) public sectors. But there are no controls over the private sector.

In Europe, the situation is markedly different. Most member countries of the European Community (EEC) have imposed data protection controls over both the public and private sectors. And Europeans are strengthening and harmonizing these controls as they plan for a unified Europe in 1992.

These developments have significant implications for Canadian firms doing business in Europe—or which hope to. Without comparable data protection laws in Canada's private sector, European countries may no longer allow companies to transfer their citizens' information to Canada. In effect, European data protection laws could become a non-tariff barrier, seriously hampering Canadian firms in their dealings with what promises to be one of the strongest trading blocks in the world.

This is no idle fear. In July 1990 the EEC issued a draft directive on protecting individuals' personal data. If adopted, it would bind all EEC member countries on January 1, 1993. The directive is designed to accomplish two broad goals.

- The first is to establish a uniform, high level of privacy protection in both the public and private sectors.

- The second is to remove all barriers to the free flow of personal data among member countries.

The directive has alarming implications for non-EEC member countries which do not measure up to the European standards. Article 24 of the draft requires members not to transfer personal data to any jurisdiction which does not ensure the data adequate protection. Given current Canadian law, it is unlikely that the private sector could prove that it adequately protects personal data.

All relevant European authorities—the OECD, the Council of Europe, the EEC and European data protectors—are fully aware of the directives's implications for countries which are not EEC members. They know that Canada (and the U.S., too) endorses data protection principles (Canada has signed the OECD Guidelines on the Protection of Personal Information). And they know that North America prefers to let the private sector police itself through voluntary compliance. But the Europeans also know that voluntary compliance has not proved particularly successful. In both Canada and the U.S. only a handful of private firms have established meaningful data protection codes of practice.

And so, while the Europeans have been willing to accept that there may be more than one way to ensure adequate data protection (voluntary codes among them), they are unwilling to compromise on the principle. There must be meaningful protection. European data protectors, the guardians of their citizens' privacy, will no longer agree to risk it by authorizing transfers of personal data to countries that pay only lip-service to data protection.

This is not a prediction hazarded on a whim. It is a summation of the comments of several European data protectors to the Privacy Commissioner.

In last year's annual report, the Privacy Commissioner recommended that Parliament amend the *Privacy Act* to require federally-regulated private sector firms to develop, file and implement privacy codes based on the internationally accepted principles established in the OECD Guidelines.

From his discussions with European data protectors the Commissioner believes voluntary codes would be acceptable—as long as they had this statutory underpinning.

Therefore, the Commissioner considers action on this recommendation is urgent. Not only do Canadians deserve this much privacy protection but, without it, Canadian firms risk labouring under a significant competitive disadvantage in their post-1992 dealings with Europe.

Hopeful beginnings

Private sector success stories should not be treated lightly simply because they are few in number. A case in point: in December 1990 the Canadian Bankers' Association (CBA) approved a model privacy code containing the minimum data protection standards member banks must apply to their customers' information.

The code provides customers with rights of access to and correction of their information. As well, it controls the banks' collection, retention, use, disclosure, disposal and security of customer records. Banks have an admirable success record in protecting customer confidentiality but now the code will give their customers greater control over their financial information.

Privacy advocates (the Commissioner among them) will find flaws. One that stands out is the code's failure to provide customers with access rights to recorded opinions or judgements about them. Only factual information will be available. Nor will the code protect employees. Nevertheless, CBA's adoption of a code must be applauded.

Another success story is Bell Canada, the largest telecommunications public utility. It too has adopted a privacy code. However, the Bell code grants privacy rights and protections to employees as well as customers. And access rights are not limited to factual data.

In an increasingly competitive telecommunications environment, Bell's tangible sensitivity to its customers' and employees' privacy is bound to have a ripple effect. The Commissioner urges other telecommunications companies to follow suit. He will monitor and report their progress.

Finally, important new privacy protections were recently announced by the Canadian Direct Marketing Association (CDMA). On February 13, 1991, CDMA launched its "Operation Integrity". CDMA has strengthened the privacy protections in its code of ethics, committing itself to giving consumers greater control over unwanted intrusions by direct mailers and telemarketers.

The program requires all CDMA members to allow consumers to opt out of their mail and phone lists. In addition, members must not include sensitive medical, financial, insurance or court information in the lists they rent. Finally, CDMA has established a task force of senior industry officials to study the privacy implications of direct marketing and to develop additional policies on transferring data.

Operation Integrity is an important step towards ensuring consumers' privacy is respected. The Privacy Commissioner appreciates CDMA's courtesy in keeping him informed and looks forward to continuing this dialogue.

Biomedical Testing

Drug testing

Regular readers of these reports will recall last year's strong cautions against resorting to widespread drug testing to wage the "war on drugs" in the federal government.

The Commissioner's in-depth study—**Drug Testing and Privacy**—examined several environments - transportation, prisons, the armed forces and athletics. Many testing programs being contemplated by the government risked violating the *Privacy Act*, the *Charter of Rights* or broader notions of the individual's integrity.

Clearly there has been some movement to protect privacy interests threatened by drug testing. The office has been consulted by Health and Welfare about drug testing protocols. It has responded to the federal government's report on drug testing in transportation. And it has discussed with the Correctional Service of Canada (CSC) its proposed regulations on drug testing in federal penitentiaries.

Transport Canada no longer proposes to conduct random mandatory drug testing for those in safety-sensitive positions. CSC's proposed regulations are an improvement over earlier ones struck down in 1989 by the trial division of Federal Court in the **Jackson** case. Health and Welfare testing protocols now contain less intrusive means of taking urine samples than did earlier proposals.

Unfortunately there are elements of the transportation drug testing policy that remain troubling. Transport Canada still intends to impose urinalysis at the time of employment, transfer and during regular medicals although its own research revealed no serious threat to safety in the industry caused by substance use. As well, urinalysis provides very limited information—that a substance has been consumed in the past—but not how often or whether the employee was impaired or, more important, is **now** impaired. Mandatory drug testing in these circumstances offends the *Privacy Act* and might not survive a challenge based on the *Charter of Rights and Freedoms*. Urinalysis should be confined to testing "for cause" or after an accident.

Regrettably, National Defence remains committed to its proposal to impose drug tests on its members. This, despite the Commissioner's recommendations and the transport committee's conclusions about random mandatory testing. DND intends to test for cause, as part of an accident or incident investigation, during a probation period following a positive test result and for data collection. It also plans random mandatory tests of members in operational or safety-sensitive positions. Unfortunately, although DND has not yet begun testing, it remains committed to the program or a modified version of it.

There is yet another concern. Fitness and Amateur Sport responded to the Dubin report on drug use among amateur athletes by setting up a new anti-doping organization funded primarily by—but not part of—the federal government. The organization will co-ordinate all sport anti-doping programs in Canada and conduct an expanded program of testing athletes for banned substances.

A major focus of the program would be “no-notice” testing of athletes outside of competition. Up to 3,000 tests could be conducted (presumably annually), the majority of which would be no-notice.

Because the anti-doping organization will not be a federal agency, it will not be subject to the *Privacy Act*. This may have been a deliberate attempt to circumvent the Act. Nevertheless, the organization’s approach (as announced by the minister) prompts some general privacy objections. Athletes may find themselves with precious few privacy rights. The Commissioner intends to discuss this situation with officials from Fitness and Amateur Sport.

The Commissioner continues to be concerned about the lack of merit of most drug testing programs. Little this office has seen in the past year has altered its thinking about the fundamental futility of testing programs and their inherent intrusiveness. The government’s example is a poor one for the private sector to follow. In most cases, the programs now contemplated or introduced by government appear not to comply with the *Privacy Act*. But public criticism of these programs is the strongest weapon this office has. It cannot enforce compliance.

HIV testing

The office’s principal work on HIV/AIDS was the 1989 report, **AIDS and the Privacy Act**. The office also contributed to developing the “Guidelines on Ethical and Legal Considerations in Anonymous Unlinked HIV Seroprevalence Research”. The guidelines were developed through meetings arranged by the Federal Centre for AIDS in late 1988 and published in the **Canadian Medical Journal** in 1990. In February 1991 the office participated in a review of the original guidelines.

In November 1990 the Commissioner’s office was represented at the meeting of the Council of International Organizations of the Medical Sciences (CIOMS), a World Health Organization body. The meeting discussed draft ethical guidelines on epidemiological research, including HIV/AIDS research. Staff continue to handle requests and investigate complaints about privacy and HIV/AIDS. Since the requests often concern issues or bodies not covered by the *Privacy Act*, the office attempts to re-direct callers to the appropriate authorities.

The office’s work on HIV/AIDS is complemented by work in Ontario. The Ontario Law Reform Commission is doing a broad study on the legal (and, to some extent, ethical) implications of HIV/AIDS testing. The Ontario Information/Privacy Commissioner has published two reports on HIV/AIDS, one dealing with HIV/AIDS and privacy, the other with HIV/AIDS and the workplace.

Genetic testing

Genetic testing is just one of many evolving biotechnologies that pose serious privacy dilemmas. Genetic testing encompasses three techniques. The first—genetic screening—examines a tissue or blood sample from an individual for genes or genetic “markers” indicating a present or potential genetic disorder or other physical trait.

The second technique is genetic monitoring. It looks for genetic or chromosomal changes that may be caused by exposure to workplace or environmental chemicals or phenomena (radiation or the fumes from plastics, for example).

The third technique is forensic DNA analysis, sometimes colloquially (and inaccurately) referred to as DNA fingerprinting. This technique matches samples of material genetically. Blood stains from the scene of a crime may be genetically matched with those of a suspect. Forensic DNA analysis may also prove blood relationships in immigration or paternity cases.

Genetic technology holds great promise for the identification of genetic disorders, a limited number of which may be treatable. However, there is a privacy concern in the potential of genetic testing to reveal highly sensitive information about the person tested and his or her genetic relatives.

Other forms of biotechnological testing, such as screening for HIV/AIDS antibodies or drugs, reveal only a single piece of information—infection with the HIV or the past use of drugs. But genetic testing can reveal hundreds of bits of information about an individual or relative. The data ranges from the certainty of developing crippling or deadly diseases (such as Huntington’s chorea or cystic fibrosis), to the likelihood of developing psychiatric disorders (manic depression) to predispositions to elevated cholesterol levels, high blood pressure or certain cancers.

Genetic testing is on the brink of becoming an issue in human reproduction (pre-conception, prenatal and neonatal testing), employment (screening and monitoring), access to government and private sector services (schooling, insurance, credit), criminal investigations, during ordinary medical care and in performing research.

The current and potential uses of the information produced by genetic testing persuaded the Commissioner to study its privacy implications. While its uses are now confined primarily to reproduction, its potential is enormous. Better that society examine the technology’s implications before it attacks privacy rights. The study should be completed by late Spring 1991.

The Commissioner has always been loathe to press for regulation of the private sector. However, the privacy implications of genetic testing demand that the government consider whether there should be direct regulation of any private sector uses of this highly intrusive technology.

The Commissioner is not alone. Privacy experts are examining similar measures in the United States. Most western European countries already regulate personal data collection by the private sector. In this sense, Canada is falling behind a growing movement to protect individual privacy not only from governments, but from the seemingly insatiable curiosity of the private sector.

Electoral Reform - A Permanent Voters' List

Privacy issues can rear their heads where least expected. A case in point was the government's appointment of a Royal Commission to determine whether Canada's electoral laws needed overhauling.

The commission was asked to examine the electoral process and party and campaign financing and to study the option of a permanent voters' list that would replace door-to-door enumeration.

Doing away with costly, time consuming door-to-door enumeration may be appealing. The process contributes to the length and expense of Canadian federal elections, but the alternative needs serious study.

The commission heard proposals which focussed on combining data from such federal data banks as income tax files, citizenship information, change-of-address notices to Canada Post, census forms and pension records. Others proposals suggested incorporating provincial health and drivers' records and there was significant support for a voter's identity card or a requirement that voters produce a Social Insurance Number.

As a result, the Privacy Commissioner wrote to the commission asking it to consider the privacy impact of its recommendations.

His concerns included the implication of new large-scale collections (or linkages) of personal information. This type of permanent voters' list would become the sort of population register that could pose a real threat to human rights and freedom. Wartime experience proves that such lists will be abused—even in Canada—to subject large groups of individuals to discriminatory treatment, arrest, detention and confiscation of their property.

Further, once in place, pressures would mount to make the list widely available to all arms of government for unrelated uses. Ensuring exclusive election use and absolute confidentiality of the data would be vital.

Growing dissatisfaction with abuses of SIN reflects public resistance to national identification and registration schemes—a resistance which would be compounded if SINs were used to link the databases and to establish a citizen's right to vote.

Finally, the *Privacy Act* prohibits access to other federal data bases to create such a list. Thus, Parliament would have to pass legislation to override the *Privacy Act*, a step the Commissioner could never support.

Citizens around the world are fed up with being counted, recorded and monitored by the state. A voters' list could evoke deep unease. It would be ironic if the electoral process—the heart of the democratic way of life—became the vehicle which tipped the scales further from the individual to the state.

While the Commissioner does not want to restrict progress, he does want to ask some pertinent questions before the project advances too far. The electoral commission has welcomed his input and plans to report to the public in the fall of 1991.

Privacy and the Public Interest: a Difficult Balance

Generally the *Privacy Act* prohibits government institutions from disclosing personal information without the subject's consent. However, the Act also recognizes 13 circumstances which dispense with this rule.

One of the 13 is very general and, hence, both difficult to apply and easy to abuse. Sub-paragraph 8(2)(m)(i) authorizes disclosure without consent:

“for any purpose where, in the opinion of the head of the institution, (i) the public interest in disclosure clearly outweighs any invasion of privacy that could result from the disclosure...”

During the past year the most frequent user of this provision was Correctional Service of Canada (CSC). The situation develops when prison incidents such as escapes, unnatural deaths or hostage takings lead to internal investigations and subsequent reports. These reports contain personal information about both the inmates and prison officials who were involved. Consequently, CSC must consider the restrictions contained in the *Privacy Act* before disclosing the reports.

CSC may want to release the reports in order to preserve public confidence in the correctional system. It may also need to provide copies to journalists who have requested access under the *Access to Information Act* or to members of Parliament or Parliamentary committees wanting to review the reports to assess overall correctional administration. In these situations, CSC removes information which is exempt under the *Access to Information Act* as well as sensitive or extraneous personal details.

CSC seeks to disclose only sufficient personal information necessary to satisfy the public interest test set out in the *Privacy Act* and give the public a clear picture of what transpired.

Once this screening satisfies the commissioner of corrections and the solicitor general, they notify the Privacy Commissioner of the intended release, in advance if reasonably possible. When the Commissioner receives the notification, he assesses whether there is a public interest disclosure which clearly outweighs any resulting invasion of privacy. If he does not agree he tells the institution. However, the Commissioner has no power to prevent the release—only to tell the individuals affected that their information will be disclosed.

Evidence of just how difficult it is to apply the “public interest” test was demonstrated in two disclosures which the Commissioner reported last year (“Reports on two inmate escapes”). The Standing Committee on Justice and the Solicitor General wanted to inquire into the events surrounding the two widely-publicized prison incidents—the escape from Dorchester, New Brunswick, of Allan Légère (during which he allegedly murdered one person) and the day-pass release from the Edmonton institution of Daniel Gingras (during which he murdered two people).

CSC had previously disclosed censored versions of the investigation reports to the media and gave that version to the justice committee. The committee, however, wanted the uncensored versions and issued an order to the solicitor general for the complete reports.

The solicitor general refused to act on the order, maintaining that the *Privacy Act* prohibited the disclosure. His refusal became the subject of a question of privilege in the House of Commons and the matter was referred to the Standing Committee on Privileges and Elections.

In his testimony before the committee, the solicitor general held that he was responsible for respecting sub-paragraph 8(2)(m)(i) of the *Privacy Act*. Therefore he had to be satisfied that a public disclosure of the reports would be in the public interest and that this interest clearly outweighed any invasion of individual privacy. He did not believe that the *Privacy Act* gave him the authority to accede to the committee's demand for an in-camera review of the uncensored reports.

The then-acting Privacy Commissioner, appearing before the privileges committee, applauded the solicitor general's resolve to protect the privacy of persons mentioned in the reports. However, he felt that the minister was taking an unnecessarily narrow view. Sub-paragraph 8(2)(m)(i) of the *Privacy Act* clearly gives the solicitor general the authority to determine whether disclosure of the uncensored reports to an in-camera session of the Justice Committee is in the public interest. The acting Commissioner maintained that it was not at all inconsistent with the provision to decide that disclosure to the committee is in the public interest, providing it takes place under conditions which would ensure that the censored portions remain confidential.

At the time of this report, the final chapter of this story has yet to be written. The privileges committee has not concluded its deliberations and the Privacy Commissioner has not completed his investigation of a related complaint.

"The truth, the whole truth and nothing but the truth"

However, there is another facet to this story. It is unusual for the Privacy Commissioner to publicly remind government institutions that privacy is not an absolute value. But the Act does recognize that privacy may be invaded in order to serve certain important, collective goods.

Being doctrinaire in insisting on confidentiality in all cases risks giving the *Privacy Act* a bad name—one it does not deserve. These CSC incident reports are a case in point.

Although the public interest CSC wants to serve (by disclosing these reports) is public confidence in the corrections system, CSC has removed portions which are critical of correctional staff members. While CSC's action to shield these individuals may be understandable, it leads to a report which gives the public a less than complete picture of the incident.

Without giving the "bad" with the "good" can CSC really be serving the public "interest"? This question is the subject of ongoing discussion between CSC and the Privacy Commissioner. What is needed, it would seem, is for CSC to use the public interest clause as an extraordinary measure and, when it is invoked, to ensure that the disclosures give the complete picture.

Complaints Directorate

Complaints have increased by approximately 10 per cent per year since the office opened for business seven years ago. This year the pattern continued as the office received 1,239 complaints compared to 1,086 last year—a 14 per cent increase.

Time limit complaints

Occasionally the Commissioner felt like a stuck record during previous reports as comments about Correctional Service Canada and National Defence delays were a recurring theme.

Now, the music has changed. Time limit complaints were down substantially this year and full credit goes to Correctional Service Canada. CSC's response to the Commissioner's criticism of last year's performance was a complete overhaul of its request handling procedures.

The result was an astounding 200 per cent decrease in new CSC time limit complaints—from 214 last year to 50 this year. Last year's volume accounted for 50 per cent of the office's delay complaints. This year's total—only 15 per cent. A tip of the hat to Correctional Service for a job well done.

Another entrenched cause of delay complaints was the Department of National Defence handling of members' Personal Evaluation Reports (PERs). The problem occurred because military personnel had to make formal application to see their evaluations and the result was a huge caseload and an inevitable backlog. Last year the Commissioner applauded National Defence's decision to treat PERs requests informally. As predicted, the number of privacy requests to DND dropped 20 per cent — most of the decrease directly attributable to the policy change. The result is a 36 per cent decline in time limit complaints against National Defence—from 78 to 50.

Clearly, government institutions are trying hard to respect the statutory time limits, the trend is evidence of that. But shrinking resources threaten the "good news" story. An individual's right to timely access to personal information should not be sacrificed on the altar of fiscal restraint.

Fair information code

Although complaints about denial of access were up, this past year's 14 per cent hike results from a substantial jump in complaints about collection, use and disclosure of personal data—the fair information code. This year's complaints against the code skyrocketed to an unprecedented 386 from last year's total of 173.

Again, labour-management disputes at Canada Post Corporation seem to be at the root of the problem. The corporation appears to be administering its new leave management policy aggressively. Employees are concerned that medical information about them has been improperly collected and used to manage attendance at work.

Top ten

This year's report includes a list of the office's top ten clients, a group which accounts for 80 per cent of its total caseload. Correctional Service Canada, the perennial leader in the new complaints category until this year, has happily ceded that honour to Canada Post Corporation.

New complaints against Canada Post went from 97 to 237, while CSC's 165 are less than half of last year's record 392.

Another significant increase occurred at Employment and Immigration Canada where the 128 complaints represented a three-fold jump. Transport Canada has returned to a more characteristic total of 67 after a low of six complaints in 1989-90. For no apparent reason National Archives, National Defence and the Canadian Security Intelligence Service have also seen significant increases while Health and Welfare and the RCMP have experienced decreases.

		GROUNDS		
DEPARTMENT	TOTAL	ACCESS	TIME LIMITS	OTHER
Canada Post Corporation	239	40	54	145
Correctional Services Canada	165	77	50	38
National Defence	163	51	56	56
Employment and Immigration Canada	128	61	44	23
Canadian Security Intelligence Service	77	67	9	1
Revenue Canada, Taxation	75	23	39	13
Transport Canada	67	43	17	7
National Archives of Canada	51	12	1	38
Royal Canadian Mounted Police	50	35	2	13
Health and Welfare Canada	32	14	15	3
Others	192	95	50	47
TOTAL	1,239	518	337	384

How institutions measured up

A number of factors—such as an unexpected volume of requests—can prompt complaints. Actually, many of the factors are beyond the control of the institutions. A more meaningful performance indicator is the proportion of complaints that are well-founded.

Using this measure, the Royal Canadian Mounted Police is the most successful institution by a long shot. Only five complaints were well-founded (or well-founded/resolved) while 16 were not well-founded and seven were discontinued. This is a decrease from 19 well-founded complaints two years ago and 10 last year. This reflects the

RCMP's sincere respect for the letter and spirit of the Act. But special kudos are due the RCMP's access and privacy coordinator for his personal commitment to reducing the number of well-founded complaints.

And National Archives continues to maintain its high standards—only four of 23 complaints were well-founded, three of which were resolved.

At the risk of appearing inconsistent, there is praise for Canada Post. Despite having the questionable honour of first place as the office's most important client, only 50 of the 230 complaints were well-founded. Of these, 37 were resolved.

		RESULTS				
GROUNDS		WELL-FOUNDED	WELL-FOUNDED RESOLVED	NOT WELL- FOUNDED	DISCONTINUED	TOTAL
ACCESS		30	70	320	16	436
	Access	27	69	305	16	417
	Correction/Notation	3	1	14	0	18
	Index	0	0	1	0	1
	Language	0	0	0	0	0
PRIVACY		17	45	141	16	219
	Collection	0	11	22	3	36
	Retention & Disposal	3	4	7	2	16
	Use & Disclosure	14	30	112	11	167
TIME LIMITS		245	0	101	23	369
TOTAL		292	115	562	55	1,024

Although CSC seems to have conquered its delay problems, it had the worst ratio of justified complaints among the large institutions as 64 per cent—103 of 162—of the complaints investigated were considered well-founded. Not far behind were Employment and Immigration and Revenue Canada Taxation with 60 per cent and National Defence with 58 per cent well-founded.

Overall, investigators completed 1,008 investigations comprising 551 not well-founded, 402 well-founded and 55 discontinued.

This year the complaints have been grouped under three major headings. They are: access complaints—dealing with individuals' problems with their applications to see personal records; privacy complaints—concerning the fair information code (proper collection, use and disclosure); and time limits—including both delay in the initial response to an application or time extensions.

More resources please!

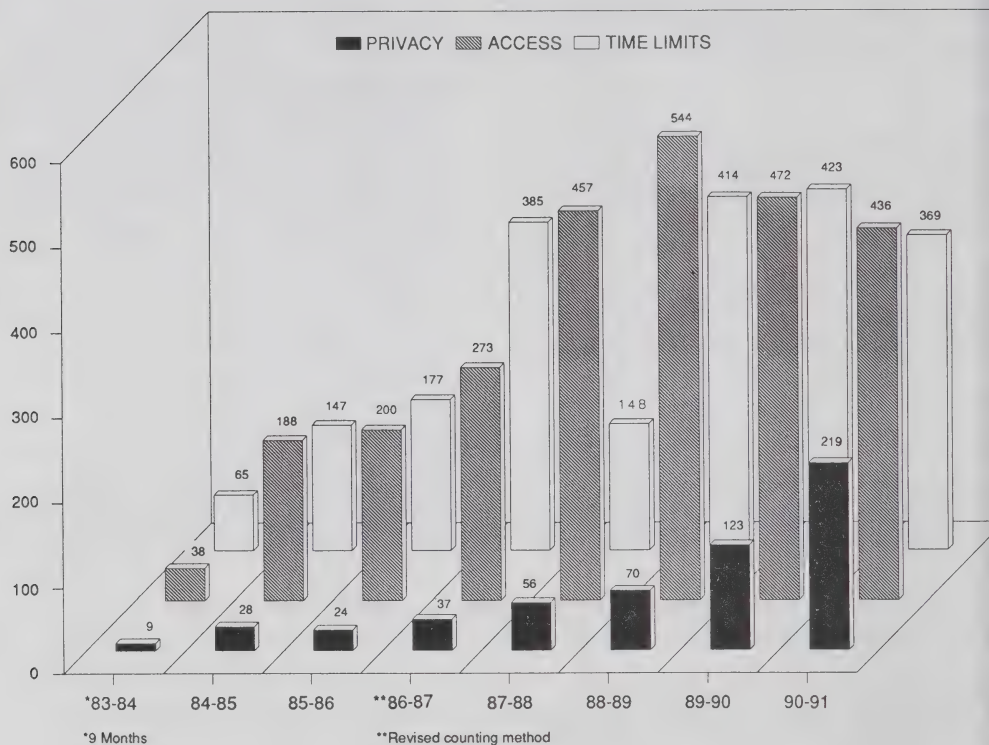
Despite having completed more than 1,000 cases, the norm for the past three years, 589 complaints were pending at the end of the year—a 38 per cent increase from the preceding year. Sadly, this means a return to the backlog the office worked so hard to eradicate two years ago. The problem will be compounded if the 10 per cent increase forecast for 1991-92 materializes—and it probably will if this year's 14 per cent increase is an indicator.

Unless the office receives more staff and money, its open caseload will soar to more than 700 complaints by the end of the current year. This represents more than the total caseload investigated by the office in the 1987-88 year.

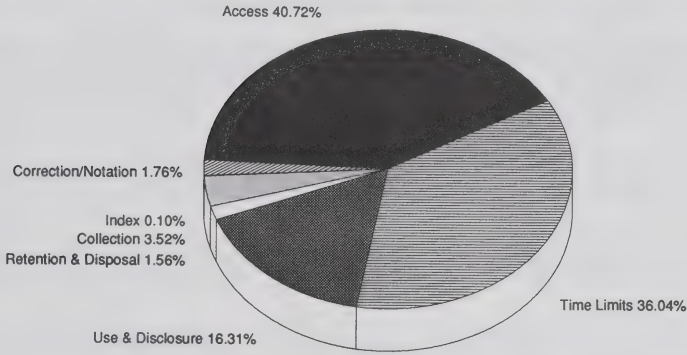
Despite increased productivity, the office has not closed more cases this year. Increased efficiency has been more than offset by the drop in time limit complaints (which consume fewer resources) and the rising tide of complaints against the fair information code (the most complex and time-consuming investigations).

Unfortunately the government turned down the office's request for more investigators and operating funds. This decision will exacerbate the ever-increasing backlog; increase investigator's caseloads and keep clients waiting longer for decisions on their complaints. In short, the office now risks becoming part of the problem.

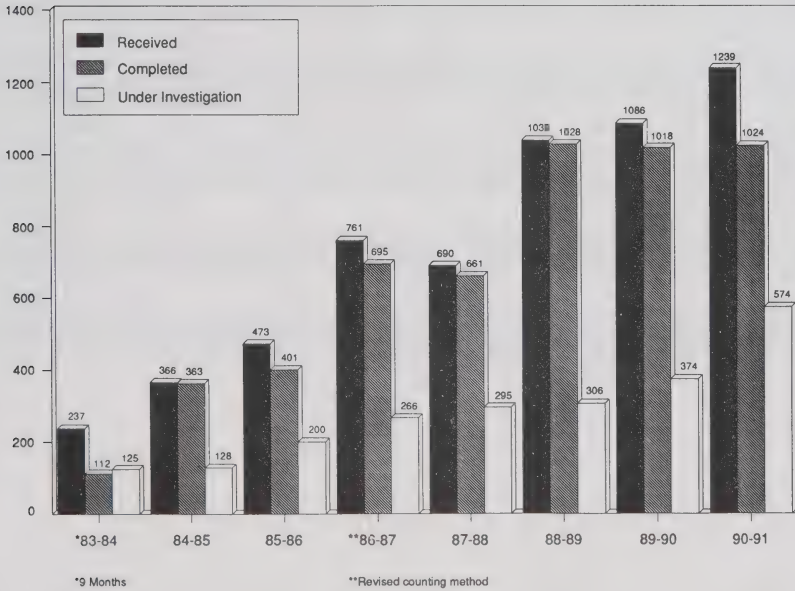
Completed Complaints and Grounds 1983-91



Complaints Completed by Grounds 1990-91



Completed Complaints 1983-91



Completed Complaints by Department and Result

Department	Total	Well-founded	Results		Disco
			Well-founded; Resolved	Not Well- founded	
Agriculture Canada	11	2	1	8	
Canada Post Corporation	233	13	39	171	
Canadian Human Rights Commission	5	1	3	1	
Canadian Security Intelligence Service	83	6	9	67	
Commissioner of Official Languages	1	0	0	1	
Consumer and Corporate Affairs Canada	5	3	0	1	
Correctional Service Canada	162	84	19	49	
Employment and Immigration Canada	78	33	10	27	
Environment Canada	1	0	0	1	
External Affairs Canada	7	3	0	3	
Farm Credit Corporation Canada	1	0	0	1	
Finance Canada	1	0	0	1	
Fisheries and Oceans	6	1	3	1	
Health and Welfare Canada	34	16	3	15	
Indian and Northern Affairs Canada	0	0	0	10	
Justice Canada	9	2	0	7	
Labour Canada	1	0	0	0	
National Archives of Canada	24	1	3	19	
National Defence	84	34	8	31	

Department	Results				
	Total	Well-founded	Well-founded; Resolved	Not Well- founded	Discontinued
ational Museums of Canada	1	0	0	1	0
ional Parole Board	20	2	5	13	0
y Council Office	3	2	0	1	0
lic Service Commission of Canada	2	0	0	2	0
lic Service Staff Relations Board	7	0	3	4	0
venue Canada, Customs and Excise	14	11	1	2	0
venue Canada, Taxation	71	43	0	28	0
ral Canadian Mint	1	0	1	0	0
ral Canadian Mounted Police	78	2	3	66	7
MP Public Complaints Commission	1	0	0	1	0
retary of State of Canada	3	2	0	1	0
citor General Canada	14	1	0	12	1
Lawrence Seaway	1	0	0	1	0
tistics Canada	1	0	0	1	0
ply and Services Canada	3	0	2	1	0
nsport Canada	42	27	2	12	1
asury Board of Canada	1	0	0	0	1
erans Affairs Canada	5	3	0	2	0
TAL	1,024	292	115	562	55

Origin of Completed Complaints

Newfoundland	0
Prince Edward Island	8
Nova Scotia	41
New Brunswick	36
Quebec	148
National Capital Region Quebec	6
National Capital Region Ontario	53
Ontario	407
Manitoba	66
Saskatchewan	33
Alberta	55
British Columbia	166
Northwest Territories	0
Yukon	5
Outside Canada	0
TOTAL	1,024

Cases

Tax files not for fan mail

A journalist got a fan letter from a federal employee at her home address and called the Commissioner's office to inquire how the admirer could have found her private residence. The journalist did not want to lodge a complaint or get the employee into trouble, but she was concerned both for her safety and how the information had been obtained.

The office was torn between respecting her wishes and ensuring that federal employees not use government files for purposes well outside the most generous interpretation of a "consistent use". The investigator tracked the source to Revenue Canada-Taxation.

Confronted with his letter, the employee explained that he simply wanted the woman's autograph. He did not appear to pose any threat to the journalist, who was relieved and asked that the case be discontinued.

However, the revelation that the employee used information from Taxation data obliged the office to tell Revenue Canada which has a strict code of ethics and imposes stringent security measures on handling taxpayers' files. Taxation investigated, found this was not the only incident and disciplined the employee.

Revenue Canada delays

Even though the *Privacy Act* has been in effect for eight years, failure to meet time limits continues to be a problem.

To name just one, Revenue Canada-Taxation occasionally displays an indifference to applicants' rights to receive their information within the time the law allows. Curious since Taxation promptly penalizes taxpayers who are casual with tax filing deadlines!

For example, on May 7, 1990, a woman went to the Vancouver taxation office to inquire about an application she had filed in January to see her income tax file. Taxation had no record of the request so she made another. On June 26, she called the Commissioner's office to complain that she had neither heard nor seen anything.

The office called Taxation to inquire. Even so, the woman did not receive the file until August 13, 96 days later. Departments are allowed to ask for a 30-day extension under some circumstances. However, they must notify the applicant who then may complain if she considers the extension unreasonable.

Revenue Canada had no justification for not writing to the woman to acknowledge her request, to say when it would provide the file and—ultimately—for not responding in time.

The Commissioner considered the complaint well-founded.

Court orders CSIS to respond

The Canadian Security Intelligence Service (CSIS) told an applicant that it could not provide the personal information he wanted in the 30 days the Act allows.

The delay was partly the result of many new applications (apparently prompted by an article in the **Toronto Star**) and by the need to consult other parties before it could release the material.

The man complained to the Commissioner and told the investigator that he intended to go to Federal Court if CSIS did not give him the information within the maximum 60 days set out in the Act.

On the 61st day, when the Commissioner found CSIS had still not finished processing the man's records, he concluded the complaint was well-founded and advised the complainant of his right to go to Federal Court. (Applicants may not ask for a court review until the Commissioner has completed his investigation.)

The complainant asked the court to issue a *Writ of Mandamus* which would compel CSIS to produce the information. The motion was heard 20 days later and the judge ordered CSIS to reply to the man's request within one month of the date of the order. CSIS complied.

Although CSIS finally provided the information, the hearing (and the extra month the court allowed) added yet another 50 days to the process — hardly a satisfactory solution. After eight years of living with the *Privacy Act*, it is unacceptable for applicants to have to go to court to force departments to provide timely access.

More access during military grievances

A complaint against National Defence (DND) may have prompted it to change its grievance procedures for military members. The case raised important questions about a member's access to factual information collected by DND's legal services during the grievance process.

At DND, lawyers may investigate military grievances to prepare legal opinions and advise the chief of defence staff. Normally, government staff relations officers (who are not lawyers) investigate such grievances. The military procedure effectively extends legal privilege over more of the documents.

The problem this causes became apparent when an officer complained to the Commissioner that DND had denied him a good deal of information from his grievance file, claiming exemptions for solicitor-client privilege or personal information about other individuals.

The investigator confirmed DND used the solicitor-client exemption on all the documents either obtained or prepared by its legal services during the grievance investigation. The department argued that the material became privileged since its legal services developed the file specifically to prepare a legal opinion and recommendations for senior staff.

The Commissioner was concerned about such a broad use of the solicitor - client privilege, considering it both unfair and contrary to the spirit of the act to use the privilege to withhold factual material and witness statements obtained during the investigation. He suggested DND use its discretion to disclose more information to the complainant. DND agreed to reconsider and gave the officer ten more pages of information including the witnesses' statements.

The Commissioner also agreed that the other disputed material was personal information about other individuals and that it was correctly exempted.

DND has since revised its military grievance procedures and now discloses to members all documents (with some limited exceptions) which the adjudicative authority will review when considering their grievances.

Can't claim exemption if doctor to disclose

A man complained to the Commissioner when National Archives denied him portions of his old military medical records, considering it to be not in his "best interest" (section 28) to examine a 25-year-old mental health assessment. National Archives was prepared, with his written consent, to give the information to his family doctor who could then explain the assessment.

Privacy regulations allow a department to require an applicant to examine personal health records only in the presence of a qualified medical practitioner or psychologist who can explain the information.

In this case, however, the man argued that he knew the contents of the assessment and did not need an explanation.

The Commissioner held that if Archives thought it was not in the applicant's best interest to see the records it should exempt them entirely. But if it intended to disclose them—even through his doctor—then it was inconsistent to claim it was not in his best interest.

The Commissioner was also concerned that Archives refused access based on a review by a psychiatrist retained to assess the file when the man submitted similar privacy requests in 1985 and 1990. The Commissioner considered the assessment unreliable since it was based solely on a review of medical files dating back 25 years and did not consider the man's current emotional state.

The information was disclosed after the Commissioner concluded that the man was entitled to see the file. Further, National Archives agreed to change its procedures for processing sensitive medical information. In future, it will either claim the medical exemption or disclose the information directly to the applicant or to his or her doctor.

Witness statements available after investigation

A woman who had lodged a discrimination complaint with the Canadian Human Rights Commission (CHRC) asked to see the information in the CHRC complaint file. She complained to the Privacy Commissioner when CHRC withheld some of the data.

What CHRC had refused to disclose was addresses and telephone numbers of other individuals and witness statements. The Commissioner agreed that others' personal information was legitimately exempt. However, he disagreed with exempting the witness statements once the investigation was completed.

Generally, the Privacy Commissioner agrees that witness statements should not be disclosed during investigations because this might harm the investigation. However, in the case at issue, the investigation was complete. The Commissioner asked CHRC to demonstrate what injury could reasonably be expected if the complainant saw the witness statements.

CHRC was unable to demonstrate any reasonable possibility that disclosure would injure either this or future investigations. Nonetheless, it took considerable persuasion before CHRC finally agreed to disclose the statements to the complainant. Since the information was initially denied, the Commissioner considered the complaint well-founded but resolved.

Revenue Canada can see personal expenses

An Ontario woman's difficulties paying her federal income tax arrears generated a complaint against Revenue Canada - Taxation. The woman was upset when an officer insisted on examining her personal expenses to assess her ability to pay. He maintained that the *Income Tax Act* gave him that right but the woman felt the procedure was abusive and an invasion of her privacy.

The *Privacy Act* limits government institutions' collection of personal information to that which "relates directly to an operating program or activity of the institution". This effectively restricts government collection to personal information which clearly is required for that program.

Revenue Canada explained that as administrators of the *Income Tax Act*, it is responsible for collecting individuals' income tax. The department has a collection procedure that ensures that the law is applied equitably to all taxpayers, but yet allows it to consider each individual's financial circumstances. In fairness to the majority who pay promptly, the department's policy deals firmly with those who do not.

The Commissioner reviewed Taxation's collection policy and agreed with the collection officer's need to examine the taxpayer's personal expenses. Under the circumstances the *Income Tax Act* requires her to provide this type of information. Thus, the Commissioner considered Taxation had respected the collection provisions of the *Privacy Act* and he concluded that the complaint was not well-founded.

Hiring must balance fairness and privacy

A complaint against Employment and Immigration Canada (EIC) demonstrated the difficulty of making the hiring process transparent without stripping away candidates' privacy.

Two successful candidates in an internal EIC competition complained that a staffing officer gave their personal evaluations and personal references to another employee who was appealing the results. This person then circulated the information in the office.

The Public Service Commission's policy on appeals requires departments to disclose only directly relevant personal information about the successful candidates. In this case the evaluations had been used during the staffing process but were neither referred to during the appeal nor considered as part of the appeal decision. Clearly they were not relevant. The disclosure was a significant invasion of the employees' privacy although the result of a perhaps overzealous attempt to be fair.

EIC reminded all its personnel divisions about the disclosure policy and will issue more detailed guidelines for staffing officers caught between the competing demands of fairness in staffing and protection of candidates' privacy.

Immigration disclosure of refugee claim "consistent"

A man wrote to the Commissioner objecting to an immigration officer having told officials of a U.S. state (without his consent) that he was claiming refugee status in Canada.

During his refugee hearing, it became apparent that the man had been found guilty of a criminal offence in a state but he had failed to appear for sentencing.

The complainant argued that since the process was not complete, his situation was not equivalent to a criminal conviction in Canada which would prevent him being considered a refugee. A senior immigration officer wrote to the clerk of the state's first circuit court to determine whether the man was considered to have been convicted. The letter explained that Immigration needed the information because the complainant had applied for refugee status.

The state court confirmed that the judicial finding of guilt was a conviction.

The investigator found that one of the objectives of the *Immigration Act* is “to promote international order and justice by denying the use of Canadian territory to persons who are likely to engage in criminal activity”. The Commissioner concluded that revealing the man’s refugee claim was permissible because it was consistent with Immigration’s purpose for having obtained the information. He considered the complaint not well-founded.

Direct pay request premature

A Transport Canada employee complained that the department was asking for his bank account number so it could deposit his pay directly, rather than issue a cheque.

Transport’s request apparently followed the federal government’s announcement that it would stop paying employees by cheque on April 1, 1991 and begin depositing pay directly into employees’ bank accounts.

The complainant objected strongly to having to give his bank account number to his employer. In fact, he was just one of a number who called or wrote to the office wanting to know if they had to provide the information.

The investigator identified two privacy issues. First, could Treasury Board (the employer) require employees to provide the location and number of their bank accounts for direct pay deposit? Did it have legal authority for collecting the information?

The Commissioner concluded that the government had the legal authority to decide how it will pay its employees. Collecting the necessary details to administer its pay procedure would not breach the *Privacy Act*.

However, the second issue concerned how the employer would deal with employees who refused to provide the information. Could it give their names, addresses and social insurance numbers to a bank to open accounts without their consent?

Privacy staff had several meetings with Treasury Board and were told that the program was still voluntary—Transport Canada had simply been eager to begin. No information had been collected except from those who had opted into the program. However, the Board acknowledged the problem of handling recalcitrant employees’ pay.

Still, with the Minister’s announcement in December 1989, it appeared that the public service was moving toward mandatory direct deposit. The Commissioner decided to hold the complaints open until the policy became clearer.

Then, on December 15, 1990, the government announced that direct deposit would remain voluntary. The complainants would not have to provide the information and the government would not be opening any accounts on employees’ behalf. Thus, the Commissioner considered the complaint not well-founded.

Staff relations board exhibits now kept two years

Although privacy regulations require government agencies to hold personal information for at least two years, a complaint revealed that the Public Service Staff Relations Board (PSSRB) kept its exhibits for just three months before having them destroyed or returned to the party who presented them.

The two-year period was written into the regulations to give individuals enough time to examine the material if they were interested.

A woman complained that her privacy rights were infringed because the PSSRB destroyed the exhibits well before the two-year period.

PSSRB explained to the privacy investigator that it lacked the facilities to keep all exhibits—items ranging from volumes of documents to a broken baseball bat, garbage cans and even a hangman's noose! PSSRB staff also pointed out that all parties to a hearing receive copies of the exhibits so nothing was being destroyed that they had not already received.

Nevertheless, the regulations are clear. The Commissioner concluded that PSSRB must keep exhibits containing personal information for at least two years after taking the last administrative action. The Board agreed and the Commissioner considered the complaint resolved.

Personal information should be accurate

A veteran Canada Post employee complained to the Commissioner that the post office had given false medical information about him to the Workers' Compensation Board (WCB), in order to deny him benefits.

Canada Post had told WCB that the employee was ineligible because his injury was caused by a chronic medical condition. According to the employee's supervisor, the employee had given her the information and she was merely reporting what she thought might be relevant to the claim.

The employee denied having the condition and a recent examination by a specialist confirmed this. He also denied ever having told anyone, let alone his supervisor, that he had the condition.

During his inquiries, the investigator noted a factor which may have contributed to the problem. Canada Post manages the WCB claims aggressively in order to minimize costs. It argues that it is obliged to give WCB any information which could question the validity of the claim.

The *Privacy Act* requires that personal information being used for administrative purposes be as accurate, up-to-date and complete as possible. In this case there was no evidence that the supervisor had made any effort to verify that the medical information was accurate.

After protracted discussions, Canada Post agreed reluctantly to tell the WCB that it had no information to substantiate its allegation that the claimant had the medical condition.

The Commissioner considered the complaint well-founded and resolved.

Licence holders list not for surveys

An airline operator's call to the office about a Transport Canada drug use survey prompted the Commissioner to initiate a complaint of his own.

The caller became concerned when a market research company asked for the names, addresses and telephone numbers of his employees. The company said it was conducting a survey for Transport Canada on substance use in the transportation industry. It needed the personal information to randomly select participants for the survey.

The surveys, it was established, were a major component of Transport Canada's study to determine what risks employee use of drugs and alcohol posed to transportation safety in Canada. Participants were asked to complete a questionnaire about their use of alcohol, prescription, non-prescription and street drugs and about workplace conditions which could influence their using these substances.

Two areas of privacy concern surfaced:

- Was there an improper collection of personal information during the survey? and
- Did Transport Canada respect the use and disclosure provisions of the *Privacy Act*?

Controls on use and disclosure require government agencies to collect only personal information that relates directly to their operating programs or activities. The information must be collected directly from the individual (whenever possible) unless that would lead to collecting inaccurate information or defeat the purpose or prejudice its intended use. And the individual must be told why the information is being collected.

The investigation established that the questionnaires contained no identifying personal information to link them to any specific individual. Since the respondents could not be identified, the information was not personal and so its collection did not violate the *Privacy Act*.

However, it was clear that Transport Canada compiled the list of some survey participants from personal information it collected for other purposes, none of which included disclosing to research organizations. In most sectors Transport gave the survey company only the names and work telephone numbers. But, in the case of airport employees, its source was a list of employees licensed to operate airside vehicles and disclosing the names was not consistent with the original collection purpose and was improper.

The investigator also found that the survey companies began collecting the information before written contracts were in place. The draft contracts contained no references to the collection principles in the Act. As a result, representatives of Privacy, Supply and Services (the contracting authority) and Transport Canada met to ensure that all future contracts requiring personal information collection contain standard clauses about collection, retention, use, disclosure and disposal of information to ensure that they comply with the Act.

The Commissioner also recommended that Transport Canada obtain the individuals' consent before considering any future use of personal information that is not consistent with the original collection purpose.

Notifying the Commissioner

During the reporting year the office examined 50 notices from government agencies advising of their intention to release personal information “in the public interest” or to benefit an individual. The disclosures ranged from confirming citizenship so that individuals could receive pensions or awards to detailed reports on escapes from federal penitentiaries. In fact, inmate incidents have become a recurring feature of the notification process (see page 24 for greater detail).

The following are examples of other public interest notifications.

DND releases security clearance details

National Defence (DND) advised the Commissioner that it intended to give an employee normally exempt information from his security clearance file.

In the midst of processing the man’s application to see his file, DND staff learned that provincial police had laid criminal charges against him, including one of sexually assaulting a former employee. His security file contained a military police interview with the plaintiff during which she detailed their longstanding sexual relationship. She had made it clear to the military police that it was mutually desired.

Since the *Privacy Act* allows investigative bodies (including military police) to protect sources interviewed during security clearance investigations, DND would normally have exempted the woman’s comments. They concerned her as well as him and it would have been virtually impossible to extricate only the man’s information from the record and the source of the comments

would have been obvious. The department’s dilemma was that it had accepted in confidence information which appeared to contradict the woman’s charges. The man may not have known about the information in his file and therefore be deprived of details vital to his defence. DND concluded it was in the public interest to provide him the information before the matter went to trial.

The Commissioner notified the woman.

Woman given details on son’s death abroad

A woman asked the RCMP and External Affairs to tell her what they knew about the death of her son in Thailand. Although both the RCMP and External had been satisfied with the Thai investigation, and a Canadian pathologist had confirmed the overseas postmortem results, the woman still had questions.

The RCMP intended to give her 21 pages from its inquiry report, exempting some limited information about other individuals. External, meanwhile, agreed to provide material from files located in two overseas embassies and Ottawa headquarters.

Normally the *Privacy Act* would protect the information—even from the man’s mother. But both agencies considered it was in the public interest to give her the report so that she could pursue her inquiries in Thailand—and perhaps put her mind at rest. The Commissioner agreed.

List of unclaimed dividends sought

An applicant used the *Access to Information Act* to ask Consumer and Corporate Affairs for lists of unclaimed dividends under three acts: the *Bankruptcy Act*, the *Canada Business Corporations Act* and the *Winding-Up Act*. The applicant intended to track down the creditors.

CCA advised the Commissioner that it would release the lists because it would benefit the individuals concerned (paragraph 8(2)(m)(ii)). The Commissioner agreed but admitted to “lingering unease about the need for this disclosure”, observing that if government institutions are reasonably able to locate individuals to whom they owe money, they should do so. He concluded that it “seemed less than ideal” to disclose personal information without consent to permit third parties to locate creditors (presumably for a fee).

Poor catch for Revenue Canada

Fisheries and Oceans advised the Commissioner that it intended to provide Revenue Canada’s GST Communications Office with a mailing list of commercial fishermen. The GST office wanted to send fishermen an information booklet explaining how they should “charge, record, calculate and send in the tax”. Revenue Canada had no other way of reaching fishermen and Fisheries concluded that clearly it was in the fishermen’s interest to receive the material.

The Commissioner was not so sure. The GST legislation had not then been passed and, while it might be helpful, he was not convinced disclosure of the list would “clearly benefit” fishermen. However, he told Fisheries he had no objection to their mailing the material for Revenue Canada.

The Fisheries department could not find sufficient “public interest” to warrant its mailing GST material. It did, however, provide Revenue Canada with a list of fishermen’s associations.

Board members’ names not “personal”

The International Development Research Centre (IDRC) told the Commissioner it would release the names of board members who had attended an IDRC meeting in Bangkok, Thailand. The centre had given a journalist (who applied under the *Access to Information Act*) the members’ expense accounts, but not the names. The journalist complained to the Information Commissioner who recommended release.

After discussing the notification with IDRC staff, the Privacy Commissioner agreed with the Information Commissioner that the board members were officers of the centre and so their expense accounts would not normally be “personal information”. However, in preparing the initial package, IDRC had provided more detail than was necessary—menu selections, insurance policy numbers, the credit cards they held and—in one case—the member’s American Express Card number.

This level of detail went beyond the requirements of public accountability. Having made the mistake, IDRC could not then withhold the names. The Privacy Commissioner accepted the notification and IDRC advised its board members of the release.

Policy and Research

Data matching

Electronic data processing poses its own threats to privacy. For example, the uncontrolled linkage of computer files could produce extensive dossiers on everyone, making a mockery of the collection restrictions set out in the Act.

To guard against this, the government introduced a data matching policy requiring that departments submit detailed proposals to the Privacy Commissioner 60 days in advance of linking databases. The policy, little more than a year old, applies a brake to untrammelled data linkage by ensuring that this independent agent (the Privacy Commissioner) weighs the proposals against a set of approved criteria. The Commissioner also acts as an advocate for those who may be affected by the match.

However, some departments seem to view the Commissioner's role as something of a rubber stamp to be applied after a last minute phone call. But Treasury Board's policy is clear — and the Commissioner's assessment is serious. Notifying the Commissioner when the system is on the launchpad will only frustrate everyone and cause delays.

This year the Commissioner's staff examined 11 proposals resulting from this policy. Following is a brief description of each match and the office's conclusions. Anyone wishing greater detail on these — or guidance on formulating their own proposals — should call the office.

Matching Employment and Immigration Canada Adjustment Assistance records with Toronto welfare files

Federal, Ontario and Toronto officials formed a committee to grapple with some of the problems caused by the increasing number of refugee claimants on Metro Toronto welfare rolls.

One of the problems was determining whether a refugee is receiving financial support from Employment and Immigration Canada's Adjustment Assistance Program. The program provides refugees with funds until they have sufficient income to support themselves or for one year, whichever comes first. Refugees benefitting from this program are ineligible for welfare.

The committee was concerned that, without some type of verification, both programs could be subject to fraudulent claims. Members agreed that EIC and Metro Toronto should share data to prevent such occurrences.

At first, EIC considered the match a "consistent use" and offered the Commissioner little substantiation. However, after a good deal of consultation, EIC provided a rationale and set out the legislative base for data sharing.

The Commissioner was satisfied but asked EIC to follow Metro Toronto's lead and tell applicants that the government agencies would verify their eligibility. He further asked EIC to add a notice and consent statement to the application forms as well as to assess whether the match reduced fraud cases enough to justify the action. EIC agreed.

External Affairs INFONNEL project

Last year's annual report said External Affairs had asked that the office examine its proposed new personnel management system which would incorporate smaller data bases into a single system with more sophisticated processing capabilities. The system would allow management to forecast, track and record all personnel actions.

Privacy staff became concerned that the proposed degree of integration might well exceed Treasury Board's approved uses of this type of database and that the proposal did not provide enough detail on system security. The staff concluded that the system design did not meet the requirements of either the *Privacy Act* or the government security policy.

Follow-up documents and discussions have failed to resolve the difficulties. Thus the office's audit branch will examine the system.

Agriculture Canada's Security Information System.

Agriculture Canada consulted the office on its plan to transfer some personal employee data from its human resource system to a security information system. Agriculture came to the office early in the process with a proposal for a "cleansing match"—one which simply verifies or updates a data base. The proposal set out the rationale for considering the transfer a "consistent use" and acted quickly to amend the bank descriptions to reflect the changes. In this example, Agriculture respected the policy and the result was a painless and speedy review.

The Personal Locator Beacon Registry

The office gave its seal of approval to a new Department of Communications system containing data on owners of "personal locator beacons". The devices are small, portable transmitters which campers, canoeists and hikers carry and activate in an emergency. The beacon transmits a radio signal to facilitate search and rescue.

Communications proposed to set up a voluntary registry containing such data as owners' names, addresses, type of vehicle and activity (land, marine or air) and next of kin. The registry, available to National Defence and the RCMP, will also be linked to DND and Transport Canada's joint search and rescue information system.

The registry is entirely voluntary and limited to this specific purpose. Participants sign a consent form and are told of the disclosures. Finally, all personal data will be stored in a newly-created personal data bank and listed in the **Info Source** guide.

Managers' new career counselling service

The office also had no difficulties with a Public Service Commission proposal to create a registry for its new confidential counselling service to help improve managers' skills.

The service is voluntary and within PSC's mandate. Participants provide the information directly and are told how it will be used. PSC will set up a bank to contain the data.

GST and SIN

A Revenue Canada notification on data linkages required by the GST has not been so clean.

Early in 1990, the Revenue minister advised the Commissioner that the GST program would involve some data matching and would use the social insurance number to register individuals and sole proprietorships. The minister assured the Commissioner that Revenue Canada took its clients privacy very seriously and promised a detailed submission "within the next few months".

Now, the legislation has been passed, detailed regulations have been adopted on sharing information and the use of SIN and still the Commissioner awaits the promised "detailed submission". In fact, only late in 1990 has the department begun to consider the data matching implications. This office has pressed for details but without success.

Fishing licence and vehicle match withdrawn

Fisheries and Oceans abandoned a project to step up fishing regulation enforcement by matching fishing licence holders with fishing vehicle permits. Fisheries withdrew the proposal when it became apparent that there was no legal justification for the match.

Immigrants' health records match

Health and Welfare Canada submitted a proposal to assess immigrants' overall health by linking its Immigration Health Services Records with provincial medical records.

The department proposed to extract statistical data only and promised not to use it for administrative purposes.

Technically this type of match does not require the Commissioner's review but the office appreciated being advised. Health care matches are a sensitive area which continue to worry the Commissioner.

Correctional Services' information gathering

CSC advised the Commissioner's office of a proposal to improve its gathering of "critical information" on persons about to be admitted to the penitentiary population. The need for better information became apparent after two recently-released federal inmates committed murders in Toronto.

When an inmate arrives at a federal facility, CSC requests information from the police, courts and various correctional and parole authorities. Agencies often do not give these requests high priority and CSC is left without critical information on which to determine the inmate's proper security level or the possibilities for parole. The problem is most acute in Metro Toronto.

As a result, CSC proposed contracting with former Toronto police officers to coordinate assembling the information.

The office examined these contracts to ensure that clauses covered contractors' collection and use of the personal information, that the collection procedure itself complied with the *Privacy Act* and that any information collected would be stored in a bank and made available to the individuals. CSC had taken all of these concerns into account.

The office noted that such release to provincial agencies might require review by the Commissioner's provincial counterparts. The staff also recommended that federal provincial agreements be drafted to cover the exchanges.

CIDA overseas student inventory

The Commissioner's office continues to struggle with a Canadian International Development Agency (CIDA) project to establish an inventory of CIDA-funded students from overseas.

CIDA's own files are organized by project or country, making it difficult to retrieve individuals' names and addresses. To solve this, CIDA proposed a tracking system that would link Employment and Immigration student authorization files which contain the information CIDA wanted. To accomplish this, it intended to send an employee to search the EIC files.

Despite privacy staff cautions that no legal authority could be found for the exchange, CIDA submitted a formal proposal. During discussions with Employment and Immigration it became apparent that their staff knew little about the proposal and — like privacy staff — could find no legal basis for this linkage. They also did not intend to comply.

As a result, CIDA asked for more consultation time and since then has submitted two different proposals. Examining the match did, however, reveal an oddity — CIDA lists no personal data banks for students and trainees in the **Info Source** guide. This was brought to the attention of Treasury Board which is responsible for ensuring government agencies comply with the *Privacy Act*.

Offsetting debts against income tax refunds

Probably one of the longest-standing data matching assessments concerns the government use of SINs to identify persons who owe money and to deduct the amounts owed from income tax refunds.

In June 1990, the Office of the Comptroller General proposed a research project to assess the usefulness of such a program to recoup some of the \$800 million owed to the Crown for overdue student loans. The office agreed to a research match but held that deductions from tax refunds should not begin without legislative amendments.

The office also wanted to be assured that money would not be deducted solely on the basis of "a hit"— simply appearing on both lists. A principle of data matching schemes requires that there be some independent verification before taking any administrative action.

These differences of opinion remained unresolved by February 1991 when the government tabled its budget. It did mention changes to allow government to recover money owing from tax refunds.

Apparently individuals will be given fair warning and special care will be taken to ensure that the deductions from refunds will not cause undue financial hardship.

Nevertheless the office maintains that this type of debt collection will require legislative amendment and not simply the mandate of the *Financial Administration Act* or claims that such behavior represents either “consistent use” of the information, or disclosure “in the public interest”.

Technology Marches On

Employment and Immigration (EIC) is at the forefront of applying new systems technology to its workplace. This fact is not surprising considering the department serves about 3,000,000 UI clients, receives some 40,000,000 claimants' reports and handles 31,000,000 inquiries each year.

Smart Cards

EIC has briefed our office on a pilot project to use "smart cards" for unemployment insurance clients. The cards resemble most bank or credit cards but are really mini computers containing 64K memory—as powerful as some of the early personal computers. Clients applying for benefits would use the card to report periods of unemployment through publicly available machines. EIC mainframe computers would then determine the claimant's eligibility, calculate the benefits and credit the payment onto the card. The claimant could then use the card to withdraw cash from an automatic teller machine or make purchases through retail direct debit machines.

The pilot project is expected to begin in two locations in the fall of 1991.

There are two clear privacy issues: ensuring that the correct person is accessing the system; and safeguarding against matching the data with other unrelated personal information.

Access appears to be controlled. Clients enter the system using a personal identification number (PIN) which they have selected. There are highly sophisticated internal security safeguards which EIC believes cannot be compromised. EIC will watch system security closely during the pilot project and brief the Commissioner.

The second concern, protecting against data linkage, has also been taken care of. Internal safeguards will prevent the card from being used for any other transactions and bank and retail machines will be limited to receiving the funds for the transaction.

However, EIC sees the single card eventually being used for as many as eight different applications. For example, cards could link the holder to an electronic job-search database describing available jobs which match their training and experience. Or they could be used to verify and pay training allowances and place the holder on training programs.

With so many possible functions, the cards could be useful for other government agencies or even private companies. EIC could sell them unused space for data or financial transactions. However, EIC recognizes that multiple uses would require segregation of the functions to prevent merging or cross-over of the data from one program to another.

Much of this project is still in the conceptual stage. EIC estimates it will take three to four years to start the UI program, another three to four years to implement and a total of 10 years for multiple applications. The scope of this project may require amendments to EIC legislation. Our office has suggested that any changes should focus on protecting the card and the transaction process, rather than simply authorizing its use.

EIC's new telephone inquiry system

The Commissioner's office remains concerned about Employment and Immigration's Automated Voice Response Enquiry System (AVRES). This pilot project allows touch telephone users to get general unemployment insurance information or details about their own claim over the phone. Callers use the phone keypad to select options and identify themselves by entering their social insurance number and date of birth. The technology permits computers to answer thousands of routine calls.

The office learned about the system when a Quebec City radio station asked us whether this was a proper use of SIN. There is no doubt that EIC can use the SIN—it was devised for the UI program. However, our office was concerned that individuals' SINs and dates of birth are so widely available that using them for identification does not restrict access to that individual.

Recognizing the weakness of SIN and date of birth, EIC looked at other solutions—client waivers, system recognition of the client's phone number or a client-chosen personal identification number (PIN), similar to bank card numbers. Although PINs appear to be the best solution, this would require a year for development and the pilot project was on the verge of launching into Ontario. With mounting internal pressure, Treasury Board approval and the system about to go to tender, EIC decided to proceed.

The Commissioner conceded that EIC was best suited to decide how to use technology to serve the public. However, he urged the department to hold off until more secure protections were in place, observing that EIC was courting the risk of embarrassment and, possible improper disclosure of a client's information.

Alas, it was too late—the project had already expanded to London and Peterborough. EIC believes the expanded pilots will enhance development and perfect a new security gate for the national system.

Consulting the Commissioner

The Commissioner's Office always welcomes opportunities to exchange information with those interested in the progress of privacy protection. Often such inquiries are outside the office's scope so it acts as a privacy clearing house, assembling material or referring inquiries to other sources. For example, research staff handled requests from Australia's new federal privacy commissioner for background on Canadian medical research guidelines, the application of federal data matching policy to law enforcement, security and intelligence data and Canada's experience with covert surveillance.

The Commissioner received other requests from down under as well. Privacy committees asked for the Commissioner's general assessment of the *Privacy Act* and his office's experience. The Australian electoral commissioner wanted information on Canadian legislative protection of whistleblowers (there is none) and Telecom Australia was interested in Canada's handling of caller ID and call management phone services, as well as codes of conduct for telecommunications companies.

The Hong Kong Secretary for Home Affairs, researching data protection legislation, needed information on registering computer systems and licensing data banks. Both these controls are features of some strict European data protection schemes—particularly the British Data Protection Act. They are not part of any Canadian legislation so his inquiry was referred elsewhere.

The Commissioner's staff also provided provincial counterparts with background information on

- federal data matching experience (Ontario);
- the privacy implications of linking health care and socio-economic records (Quebec).

The staff also assembled the latest federal material on informatics applications of government databases and a management framework for disseminating corporate affairs databases. This was in response to a request from the Ontario Ministry of Consumer and Commercial Relations for information on the privacy implications of public data bases.

The Royal Commission on New Reproductive Technologies asked the Privacy Commissioner for input on the privacy implications of the new reproductive techniques. The Commissioner intends to make a submission once the genetics study is complete. In the meantime, he welcomed the consultations.

Inquiries

Inquiries to the office continue to climb. Inquiries officers handled 4,032 calls and letters, compared with 3,447 the previous year—an increase of 17 per cent.

Fifty-five per cent of the inquiries concerned the use of or interpretation of the Act. Here are some examples: Canada Post employees asked whether they had to sign a consent to release their medical records to the employer; inmates questioned whether penitentiaries could open their mail; and Transport Canada's privacy office wanted to know whether a person's voice (on an audio tape) is considered personal information. In each case, the inquirers were referred to Treasury Board or the Department of Justice for interpretation.

The second largest inquiry category—17 per cent—comprised calls about privacy problems outside the Commissioner's jurisdiction. Four per cent of these inquiries concerned federal agencies and Crown corporations not covered by the Act. In one instance, a correctional officer was upset because he was shown on a CBC telecast. Apparently the cameraman had assured him he was not filming but simply adjusting the lens. The man worried that appearing on camera could endanger his life and that of other guards who are sometimes threatened by inmates. Since CBC is not covered by the Act, the office could offer no help.

The other 13 per cent of these inquiries were about other levels of government or—frequently—the private sector. For example: A woman called to enquire about a job application given her by the Canadian Imperial Bank of Commerce (CIBC). The form asked for consent to disclose personal information from credit agencies and former employers and included a statement that “permission includes my consent to the release of personal information concerning me within the meaning of subsection 8(2) of the *Privacy Act*”.

This puzzled the Commissioner's staff on two counts:

- the banks are not subject to the Act; and
- section 8 says that government may not disclose personal information without the individual's consent.

The subsection cited describes the exceptions to the rule, none of which could be remotely interpreted as including release to prospective employers!

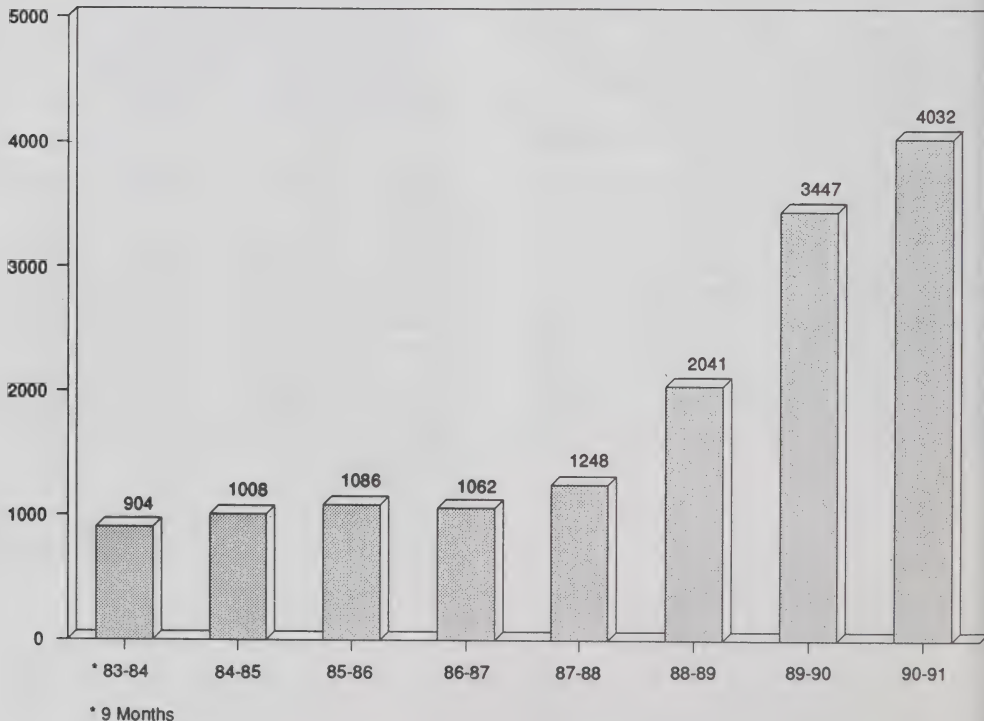
Staff concluded that the statement had no legal effect and did not dilute the protection of information held by the federal government. Legal counsels for both the office and CIBC discussed the consent, but, without jurisdiction, the Commissioner could not have the reference removed. And the bank has not apparently done so voluntarily since the office has received another complaint.

The most frequent Social Insurance Number (SIN) complaints (13 per cent of inquiries) cite insurance companies, video rental outlets, banks, grocery and department stores. Callers are amazed and unhappy that restrictions on uses of the SIN apply only to the federal government.

Several callers focused their anger on the Royal Bank's Gold Card application. The agreement requires applicants to consent to a blanket collection and disclosure of the SIN if they supplied it "in any application" to the bank. The office is inquiring whether opening a bank account (for which customers must supply a SIN under the Income Tax Act) is "an application".

Finally, eight per cent of inquiries were unrelated. A number of these deal with applying for a pardon and they are referred elsewhere. But many are from frustrated taxpayers who find in the office's toll-free line an opportunity to talk to a real person who works for "The Government".

Inquiries 1983-91



Compliance Directorate

The directorate's objectives for 1990-91 included auditing three major institutions, evaluating and improving the audit process and product, developing a privacy awareness component to audits and establishing an effective audit process for personal information held in electronic data processing (EDP) systems.

The office selected National Defence, the Royal Canadian Mounted Police and External Affairs, three institutions which hold the most sensitive and wide-ranging banks of personal information and operate some of the most sophisticated information handling systems in the country. While the war in the Persian Gulf and the Oka crisis at home had a serious impact on the success of the planned audit program, staff completed auditing the RCMP and DND and issued an interim report for External Affairs.

Due to the logistical problems and expense associated with international travel, the office has deferred its audit of External's overseas operation and the detailed review of its international information processing systems.

These agenda changes meant that the office could begin three smaller audits late in 1990; the National Capital Commission, the Office of the Comptroller General and the Commissioner of Official Languages. One of these, the Commissioner of Official Languages, was completed by year end.

The directorate now offers a "privacy awareness component" as part of its audits. Audit teams provide on-site presentations on the *Privacy Act* and have available two video cassettes which graphically illustrate the concerns pursued in the compliance audit. The videos are used only when the client institution chooses to become more informed.

All this year's investigations included an improved audit of information in computer systems. These new procedures and processes were used at DND, the RCMP and the Office of Comptroller General (OCG). In fact the OCG audit focussed entirely on EDP. Experience gained in these investigations will result in production of specific manuals and guides for this audit component.

The office was also involved in the following special investigations or projects:

- Cellular phone spectrum searching by the RCMP;
- CSIS establishment of an exempt bank;
- Indian Affairs and Northern Development (DIAND) internal audit;

-
- concerns about upward evaluation in Industry, Science & Technology and DIAND;
 - the request for the release of Bell Canada technical information to the Criminal Intelligence Service of Ontario.

AUDIT FINDINGS

Royal Canadian Mounted Police

The audits to date have shown that the RCMP in particular has made a concerted effort to ensure that it complies with the *Privacy Act*. It has made privacy considerations a high priority, undertaking periodic information sessions at all levels and introducing training on the *Privacy Act* as part of the curriculum both for new recruits and officer trainees.

Although auditors found instances where personal information holdings were not adequately described in the Personal Information Index (now **Info Source**), these were due either to oversights or to descriptions not keeping pace with changes in operating procedures.

Some records containing personal information were not being disposed of in accordance with approved schedules and Privacy Regulations. This was particularly true with the disposal of performance logs (a type of manager's diary to record employees' daily performance). The logs were the subject of numerous meetings between privacy staff and RCMP privacy personnel, all seeking a solution that would satisfy both the privacy requirements and the force's administrative needs.

The audits found some instances of personal information not being adequately protected against unauthorized disclosure. The most serious involved the Victims Assistance Program where auditors found that volunteer counsellors have been given access to complete investigation files.

Two areas of particular interest examined during the RCMP audit were facsimile (FAX) transmission and using micro-computers to handle personal information. It is a pleasure to report that the RCMP has specific policies and procedures on transmitting personal information by FAX and handling it by micro-computer. These controls ensure that sensitive personal information is transmitted only through the RCMP's own secure communications facilities. Auditors inspected a number of computer systems and found evidence that the personal information they contained was properly protected.

National Defence (DND)

The office has reported its detailed findings to National Defence and is awaiting management's response. The practice is not to describe audit findings publicly until staff have had an opportunity to examine the department's comments and discuss any areas that may be in dispute.

Other audits

Other audits disclosed that retention and disposal standards are not always upheld or are inadequate. There was evidence that personnel files are not generally disposed of on time and some personal information banks have indefinite retention periods. Some third party information, which could be inadvertently disclosed, is found on personnel files. Sensitive and inappropriate information is often found on some personnel files and the need-to-know principle is not in place in most institutions. The security for personal information held by many institutions is inadequate, while descriptions for many information banks are inaccurate.

In fairness, however, most personnel expressed interest not only in the audit objectives but also in the proper application of the *Privacy Act* throughout their institutions. In a number of cases staff corrected problems before the privacy investigators left.

Among smaller institutions with fewer resources to spend on applying the Act, there tend to be greater opportunities for inappropriate handling of personal information. Policies and procedures tend to be out of date or absent and general knowledge of the Act is consistently lower than in the major departments. The security of personal information collected by these institutions is usually at risk.

So it is refreshing to report on a smaller institution which generally handles personal information in accordance with the *Privacy Act*.

Office of the Commissioner of Official Languages

Throughout the audit of the Office of the Commissioner of Official Languages it was evident that although most employees had only a cursory knowledge of the *Privacy Act*, all had a high degree of concern for the proper management of personal information. Auditors agreed that this concern reflected the provisions in the *Official Languages Act* dealing with the confidentiality of complaint investigations.

Yet, there were instances of personal information not being adequately protected against unauthorized disclosure and in one case, the computer system's security features had been rendered inadequate due to improper administration and protection of passwords.

Common findings

Overall, some of the most common observations in all audits were:

Inadequate protection of personal information

- Managers, supervisors and other employees are allowed to see personnel files for routine administrative purposes. Records staff have access to their own and each others' personnel file, allowing them to see sensitive personal information for which they have no "need-to-know". (e.g. - Personal History Forms, results of credit and reference checks, medical diagnosis, details of family members, designation of beneficiary, Canada Savings Bonds purchases, United Way contributions, etc.)

-
- Some files contained a limited amount of third-party personal information, usually when the subject's name is on a list with other employees, often including everyone's Social Insurance Numbers.
 - Usually personal information handled by microcomputers is not adequately protected either by external security provisions (keyboard locks, hard disc protection, etc.) or internal protection (accounts, IDs, passwords, partitions, backup, etc.).
 - File jackets tend to bear the particulars of an individual along with the caption of the file. This is especially pertinent where the file relates to investigations, complaints or special requests. For example, one personal file jacket included notations about a sexual harassment allegation, including the victim's name. The information was clearly visible to mail clerks or anyone who saw the file on a desk.

Improper disclosure of personal information

- Personnel records often contain documents that should have been purged from the file or retained on other files. Individuals' medical information and security-related material are found in up to 10 per cent of the records sampled.

Misuse of personal information

- Information properly collected for specific purposes is sometimes used for follow-on purposes (e.g. personal harassment files used for grievance and discrimination cases).

Improper retention and disposal

- Many banks have improper retention and disposal schedules and proper schedules are not being maintained.

Corporate Management

Corporate Management provides both the Information and Privacy Commissioners with financial, personnel, administrative, informatics and library services.

Finance

The Offices' total resources for the 1990-91 fiscal year were \$6,372,000

and 78 person-years, an increase of \$567,905 and three person-years over 1989-90. Personnel costs of \$4,897,442 and professional and special services expenditures of \$577,300 accounted for more than 87 per cent of the total. The remaining \$852,060 covered all other expenses.

The following are the Offices' expenditures for the period April 1, 1990 to March 31, 1991*

	Information	Privacy	Corporate Management	Total
Salaries	1,685,327	1,856,590	652,525	4,194,442
Employee Benefit Plan Contributions	288,230	323,380	91,390	703,000
Transportation and Communication	38,141	114,167	123,309	275,617
Information	84,446	58,546	5,549	148,541
Professional and Special Services	411,801	130,150	35,349	577,300
Rentals	3,952	2,214	11,413	17,579
Purchased Repair and Maintenance	14,628	3,919	9,676	28,223
Utilities, Materials and Supplies	9,847	14,978	30,655	55,480
Acquisition of Machinery and Equipment	176,236	51,508	85,672	313,416
Other Payments	6,145	3,475	3,584	13,204
TOTAL	2,718,753	2,558,927	1,049,122	6,326,802

* Expenditure figures do not incorporate final year-end adjustments reflected in the Office's 1990-91 Public Accounts.

Personnel

An increase of three person-years and a change of both the Privacy and the Information Commissioners contributed to an active personnel program. There were 45 staffing actions, including outside recruitment, promotions, the hiring of term employees and some reclassifications.

Administration

New space was fitted-up for occupancy in the fall of 1990 and some progress was achieved in the records management area, particularly in the scheduling of administrative records.

Informatics

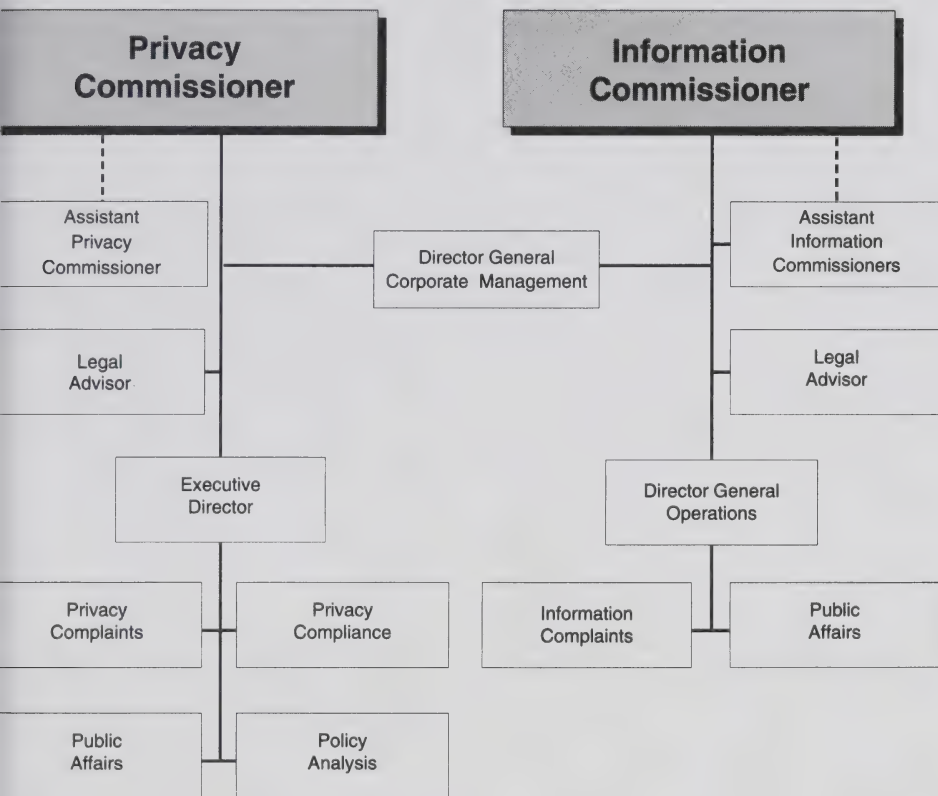
A new information technology was introduced to the organization. Three studies were undertaken concerning case management systems, additional office automation and networking in a secure environment. These studies will be completed in 1991-92 and will provide the necessary information to form a long-term information technology plan.

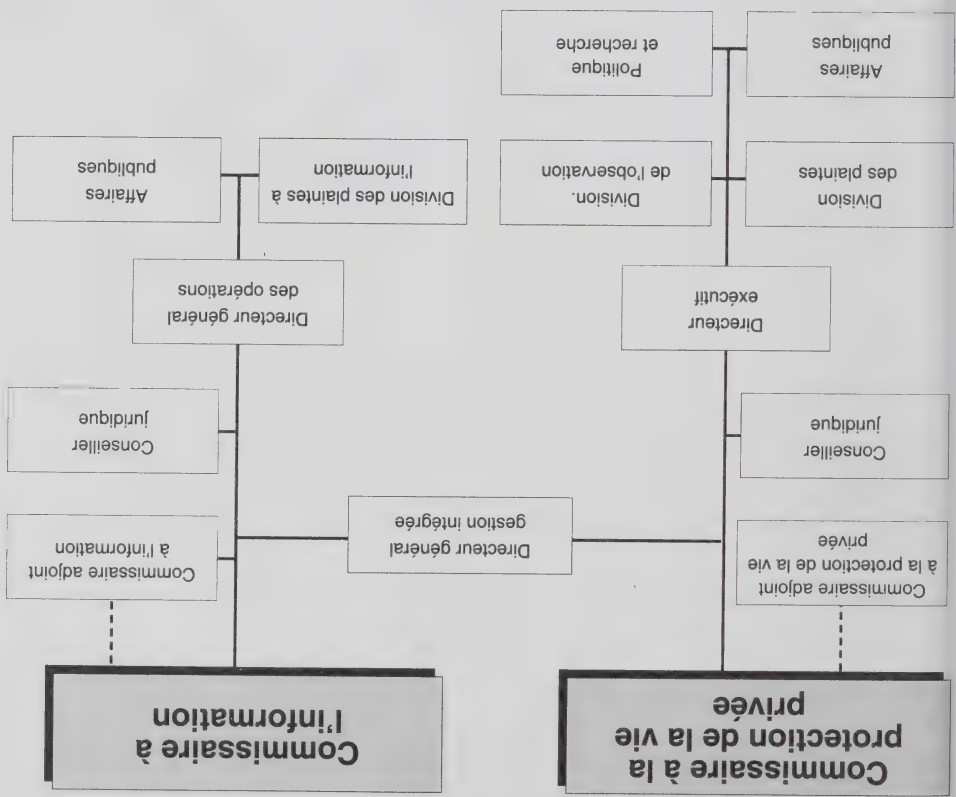
Library

The library provides services to the Information and the Privacy Commissioners. It is a resource centre for both the Information and Privacy staffs which is also open to the public.

A total of 436 books, periodicals, and annual reports were acquired through the Government Depository Services program. There were 835 items loaned and 847 reference questions answered. The automation of library functions was completed this year.

Organization Chart





Etat des dépenses des Commissariats
pour la période du 1^{er} avril 1990 au 31
mars 1991*

Personnel

Les services de la bibliothèque sont à la
disposition des deux commissaires ainsi
que de leur personnel, mais le public y a
aussi accès.

Bibliothèque

Les nouvelles acquisitions, effectuées
grâce au Service du Programme de
dépot, totalisent 436 livres, périodiques
et rapports annuels. La bibliothèque a
prêté 835 ouvrages et répondu à 847
questions grâce à son service de
référence. De plus, l'automatisation de
ses services a été menée à bien.

Avec une augmentation nette de
l'effectif de trois années-personnes et la
nomination d'un nouveau Commissaire
à la protection de la vie privée et d'un
nouveau Commissaire à l'information, le
programme du personnel a été fort
occupé. Le nombre de mesures de
dotation s'est élevé à 45, ce qui
comprend les activités de recrutement
externe, les cas d'avancement,
l'embauchage de personnes nommées
pour une période déterminée et certains
cas de reclassement.

Administration

De nouveaux locaux ont été aménagés
à l'automne de 1990, et certains progrès
ont été accomplis dans le domaine de la
gestion des documents,
particulièrement pour l'établissement de
calendriers de traitement des dossiers
administratifs.

Informatique

Une nouvelle infrastructure informatique
a été introduite. Le personnel a
entrepris trois études, l'une sur les
systèmes de gestion des affaires, l'autre
sur la bureautique et la dernière sur les
façons de travailler en milieu protégé.
Les trois études seront menées à bien
en 1991-1992 et produiront l'information
nécessaire pour l'élaboration d'un plan
à long terme de technologie
informatique.

La gestion intégrée fournit au Commissariat à l'information et au Commissariat à la protection de la vie privée des services en matière de finances, de personnel, d'administration, d'information et de bibliothèque.

Finances

Le budget total des deux Commissariats pour l'année financière 1990-1991

s'élevait à 6 324 000 \$. L'effectif global était de 78 années-personnes. Les augmentations étaient respectivement de 468 000 \$ et de trois années-personnes par rapport à 1989-1990. Les dépenses engagées au titre du personnel (4 498 218 \$) et des services professionnels et spéciaux (577 300 \$) représentent plus de 87 p. 100 du total des dépenses. Le reste, soit 852 089 \$, a couvert tous les autres frais.

Ci-dessous les dépenses des commissariats pour la période allant du 1^{er} avril 1990 au 31 mars 1991*

	Information	Vie privée	Gestion intégrée	Total
Salaires	1 685 327	1 856 590	652 525	4 194 442
Contributions aux régimes d'avantages sociaux des employés	288 230	323 380	91 390	703 000
Transports et communications	38 141	114 167	123 309	275 617
Information	84 446	58 546	5 549	148 541
Services professionnels et spéciaux	411 801	130 150	35 349	577 300
Locations	3 952	2 214	11 413	17 579
Achats de services de réparation et d'entretien	14 628	3 919	9 676	28 223
Services publics, fournitures et approvisionnements	9 847	14 978	30 655	55 480
Acquisition de machines et d'équipement	176 326	51 508	85 672	313 416
Autres dépenses	6 145	3 475	3 584	13 204
TOTAL	2 718 753	2 558 927	1 049 122	6 326 802

* Les dépenses n'incluent pas les ajustements de fin d'année reflétés dans la section des comptes publics 1990-1991 traitant des commissariats.

- Les périodes de conservation et les calendriers de retrait de nombreux fichiers ne sont pas conformes aux règles et ne sont pas respectés.
- Conservation et retrait insatisfaisants**

- Les renseignements personnels recueillis légalement à des fins précises sont parfois utilisés ensuite à d'autres fins (p. ex., des dossiers de harcèlement personnel utilisés dans des cas de griefs et de plaintes de discrimination).

Utilisation abusive des renseignements personnels

- Les dossiers du personnel contiennent souvent des documents qui auraient dû être carrément retirés, ou conservés dans d'autres dossiers. Les vérificateurs ont trouvé des renseignements médicaux ainsi que de l'information liée à la sécurité dans quelque 10 p. 100 des dossiers examinés.

Divulgaration abusive de renseignements personnels

- Les chemises contenant les dossiers tendent à porter une inscription contenant des détails sur l'intéressé en plus du titre du dossier. C'est particulièrement important lorsqu'il s'agit d'un dossier d'enquête ou de plainte, ou encore d'une demande spéciale.

Conclusions similaires

Globalement, l'exercice s'est soldé par une série d'observations communes à la plupart des vérifications.

Protection insuffisante des renseignements personnels

- Les cadres, superviseurs et autres employés sont autorisés à consulter les dossiers du personnel à des fins administratives courantes. Les préposés aux dossiers ont accès à leurs propres dossiers du personnel ainsi qu'à ceux de leurs collègues, ce qui leur donne la possibilité de prendre connaissance de renseignements personnels dont ils n'ont pas besoin pour leur travail (formules d'antécédents personnels, résultats des vérifications du crédit et des références, diagnostics médicaux, renseignements sur les membres de la famille, noms des bénéficiaires, achats de Bons d'épargne du Canada, contributions à Centraide, etc.).
- Certains dossiers de ce Commissariat contiennent quelques renseignements personnels sur des tiers, habituellement quand le nom de la personne visée figure avec ceux d'autres employés sur une liste où l'on trouve souvent le numéro d'assurance sociale de chacun.
- Les renseignements personnels traités par micro-ordinateurs ne sont généralement pas assez bien protégés, que ce soit par des moyens externes (verrouillage des claviers, protection du disque rigide, etc.) ou internes (comptes, codes d'identité, mots de passe, cloisonnements, sauvegardes, etc.).

Dans les petites institutions, qui ont moins de ressources que les grandes à consacrer à l'application de la Loi, il semble qu'on risque davantage de traiter incorrectement les renseignements personnels. Les renseignements et procédures ont tendance à être désuètes ou totalement absentes, et le niveau global de connaissance de la Loi est toujours plus bas que dans les grands ministères et organismes. La sécurité des renseignements personnels recueillis par ces institutions est donc habituellement compromise.

C'est pour cette raison que nous sommes heureux de faire état de nos conclusions sur une petite institution qui traite généralement ses renseignements personnels conformément à la Loi.

Commissariat aux langues officielles

Durant toute notre vérification au Commissariat aux langues officielles, il était évident que, même si la plupart des employés n'avaient qu'une connaissance sommaire de la Loi sur la protection des renseignements personnels, tous étaient bien décidés à gérer convenablement les renseignements de ce genre. Les vérificateurs estiment d'ailleurs que ce souci reflète l'importance que la Loi sur les langues officielles accorde à la confidentialité des enquêtes sur les plaintes.

Néanmoins, les renseignements personnels que ce Commissariat détient ne sont pas toujours bien protégés contre leur divulgation non autorisée, et, dans un cas, la protection du système informatique laissait à désirer en raison d'une gestion et d'une protection insatisfaisantes des mots de passe.

Autres vérifications

Les autres vérifications ont révélé, une fois de plus, que les normes de conservation et de retrait des renseignements personnels ne sont pas toujours respectées, voire qu'elles sont carrément insatisfaisantes. Les vérificateurs ont constaté que les dossiers du personnel ne sont généralement pas retirés en temps voulu, et que certains fichiers de renseignements personnels sont conservés indéfiniment. Les fichiers du personnel contiennent des renseignements sur des tiers qui risquent d'être divulgués par inadvertance. En outre, on trouve souvent dans certains fichiers du personnel des renseignements de nature délicate (ou non pertinents). Qui plus est, dans la plupart des institutions, le principe du « besoin de savoir » n'est pas appliqué. Beaucoup d'entre elles n'ont pas de méthodes de sécurité satisfaisantes pour protéger les renseignements personnels qu'elles détiennent, et la description de nombreux fichiers est incorrecte.

En toute justice, il faut reconnaître que la plupart des personnes rencontrées dans le contexte de nos vérifications ont dit s'intéresser non seulement aux objectifs de la vérification elle-même, mais aussi à une bonne application de la *Loi sur la protection des renseignements personnels* dans l'ensemble de l'institution à laquelle elles appartiennent. Dans plusieurs cas, les responsables ont même remédié aux problèmes avant le départ de nos vérificateurs.

La vérification a révélé deux secteurs particulièrement intéressants, à savoir la transmission par télécopieur et l'utilisation de micro-ordinateurs pour le traitement des renseignements personnels. Nous sommes heureux de pouvoir conclure que la GRC s'est donnée une politique et une procédure de transmission de renseignements personnels par télécopieur et de traitement de ces renseignements par micro-ordinateurs. Grâce aux mécanismes de contrôle en place, la Gendarmerie ne peut transmettre des renseignements personnels de nature délicate que par l'intermédiaire des systèmes Comsec, d'une sécurité éprouvée. Les vérificateurs ont inspecté plusieurs systèmes informatiques utilisés par la GRC et ils ont constaté que, dans chaque cas, les renseignements personnels étaient bien protégés.

Ministère de la Défense nationale (MDN)

Le Commissariat a communiqué ses constatations détaillées au MDN, et il attend ses commentaires. Normalement, il ne rend pas ses constatations publiques avant que son personnel ait eu l'occasion d'étudier les commentaires de l'institution faisant l'objet de la vérification et de discuter de tous les points litigieux.

Les vérificateurs ont constaté que, dans certains cas, les renseignements personnels détenus par la GRC n'étaient pas décrits convenablement dans le Répertoire des renseignements personnels (le nouvel InfoSource), mais il convient de souligner que ces lacunes étaient imputables à des oublis ou au fait que les descriptions n'avaient pas été modifiées pour refléter l'évolution des méthodes de fonctionnement de la Gendarmerie.

Certains dossiers contenant des renseignements personnels n'ont pas été retirés conformément aux calendriers établis et au règlement sur la protection de ces données. C'était particulièrement manifeste dans le cas des registres du rendement; ils ont fait l'objet de nombreuses rencontres entre le personnel du Commissariat et les responsables de la protection de la vie privée à la GRC, qui se sont tous efforcés de trouver une solution satisfaisant à la fois aux exigences de protection de la vie privée et aux contraintes administratives de la GRC.

Les vérificateurs ont jugé que, dans certains cas, les renseignements personnels n'étaient pas suffisamment bien protégés contre une divulgation non autorisée. Le cas le plus grave était celui du programme d'aide aux victimes, car les vérificateurs ont constaté que des conseillers bénévoles avaient eu accès à des dossiers d'enquête complets.

La Direction a aussi participé aux enquêtes ou projets spéciaux suivants :

- recherches sur toute la gamme des fréquences des téléphones cellulaires par la GRC;
- établissement par le SCRS d'un fichier inconsultable;
- vérification interne au ministère des Affaires indiennes et du Nord (MAIN);
- préoccupations soulevées par l'évaluation inversée au ministère de l'Industrie, des Sciences et de la Technologie ainsi qu'au MAIN;
- demande de divulgation des renseignements techniques détenus par Bell Canada au Service des renseignements (criminels) de l'Ontario.

CONSULTATIONS

Gendarmerie royale du Canada

Jusqu'à présent, les vérifications ont démontré que la GRC se distingue par la qualité de ses efforts concertés en vue de respecter la Loi sur la protection des renseignements personnels. En effet, elle accorde une priorité à ces questions, en organisant régulièrement des séances d'information à tous les niveaux et en incorporant une introduction à la Loi sur la protection des renseignements personnels au programme d'études des nouvelles recrues et des agents en formation.

En 1990-1991, la Direction avait pour objectifs de faire des vérifications dans trois grandes institutions fédérales, d'évaluer et d'améliorer sa procédure de

vérification - et la qualité de ses vérifications - , d'ajouter à sa démarche une sensibilisation des institutions à la protection de la vie privée et de mettre au point une méthode de vérification efficace à l'égard des renseignements personnels stockés dans des systèmes de traitement électronique des données.

La Direction a fait les trois vérifications qu'elle avait prévues, à la Défense nationale, à la Gendarmerie royale et aux Affaires extérieures, des institutions dont les banques de données contiennent des renseignements personnels très délicats et qui comptent parmi les plus complètes et les plus perfectionnées du Canada. La guerre du Golfe et la crise d'Oka ont quelque peu retardé les vérifications prévues au MDN et à la GRC, mais le personnel a quand même pu les mener à bien, en plus de produire un rapport provisoire sur la plus grande partie de la vérification réalisée aux Affaires extérieures.

En raison des problèmes logistiques et des frais de voyage considérables qu'elle aurait entraînés, la Direction a reporté sa vérification des activités des Affaires extérieures à l'étranger ainsi que son examen détaillé des systèmes de traitement de l'information internationale du Ministère. Ces modifications du calendrier de travail ont permis à la Direction d'entreprendre vers la fin de 1990 trois vérifications de moins grande envergure, l'une à la Commission de la capitale nationale, une autre au Bureau du Contrôleur général et la troisième au Commissariat

aux langues officielles; seule la troisième était menée à bien à la fin de l'exercice. Comme prévu, la Direction a ajouté à ses vérifications un volet de sensibilisation des institutions à la protection de la vie privée. Les équipes de vérification offrent dans les locaux des institutions visitées une explication de la Loi sur la protection de la vie privée étayée par la présentation de deux cassettes vidéo qui donnent une excellente idée de ce qu'elles cherchent à faire dans leurs vérifications. (Ces vidéos ne sont utilisées que si l'institution veut plus d'information.) Toutes les vérifications de cette année ont compris une analyse améliorée des renseignements stockés dans les systèmes informatiques. Les nouvelles méthodes et la nouvelle approche ont été employées au MDN et à la GRC, ainsi qu'au Bureau du Contrôleur général. Dans ce dernier cas, la vérification a porté exclusivement sur le traitement électronique des données. L'expérience acquise rendra possible la production de manuels et de guides sur cet aspect de la vérification.

Plusieurs de nos correspondants se sont dits très mécontents de la formule de demande de Carte d'or de la Banque royale, qui exige leur consentement à une collecte illimitée de renseignements et à la divulgation de leur NAS (s'ils l'ont déjà donné à la Banque dans une demande quelconque). Le Commissariat aimerait savoir si le fait d'ouvrir un compte bancaire constitue une «demande», étant donné que les clients doivent donner leur NAS à cette fin, conformément à la Loi de l'impôt sur le revenu.

Enfin, 8 p. 100 des demandes de renseignements n'ont aucun lien commun, si ce n'est que bon nombre d'entre elles concernent une éventuelle demande de pardon; celles-là sont renvoyées ailleurs. Une grande partie des autres proviennent de contribuables frustrés qui profitent de la possibilité d'appeler sans frais au Commissariat afin de pouvoir parler avec quelqu'un qui travaille pour le «Gouvernement».

Le personnel du Commissariat a dû vraiment se creuser la cervelle, d'abord parce que les banques ne sont pas assujetties à la Loi, puis parce que l'article 8 de la Loi dispose que les institutions fédérales ne peuvent pas communiquer de renseignements personnels sans le consentement de l'individu concerné. Le paragraphe mentionné dans la formule de la Banque précise les exceptions à la règle, mais aucune d'entre elles ne saurait être interprétée, même en étant tirée par les cheveux, comme autorisant la divulgation de ces renseignements à des employeurs éventuels!

Le Commissariat a conclu que l'attestation n'avait aucune valeur légale et ne réduisait nullement la protection des renseignements détenus par l'administration fédérale. Les conseillers juridiques du Commissariat et de la Banque ont discuté du consentement demandé par cette dernière, mais le Commissaire n'a pas pu faire retirer la déclaration contestée de la formule, étant donné qu'il n'a pas compétence dans le secteur bancaire. La Banque n'a hélas pas retiré la déclaration de son plein gré, car le Commissariat a reçu une autre plainte à cet égard.

Les demandes de renseignements les plus fréquentes au sujet du numéro d'assurance sociale (NAS) - 13 p. 100 de l'ensemble - concernent des compagnies d'assurance, des comptoirs de location de vidéos, des banques, des épiceries et des magasins à rayons. Nos correspondants sont à la fois étonnés et déçus de se faire dire que les utilisations du NAS ne sont limitées que dans l'administration fédérale.

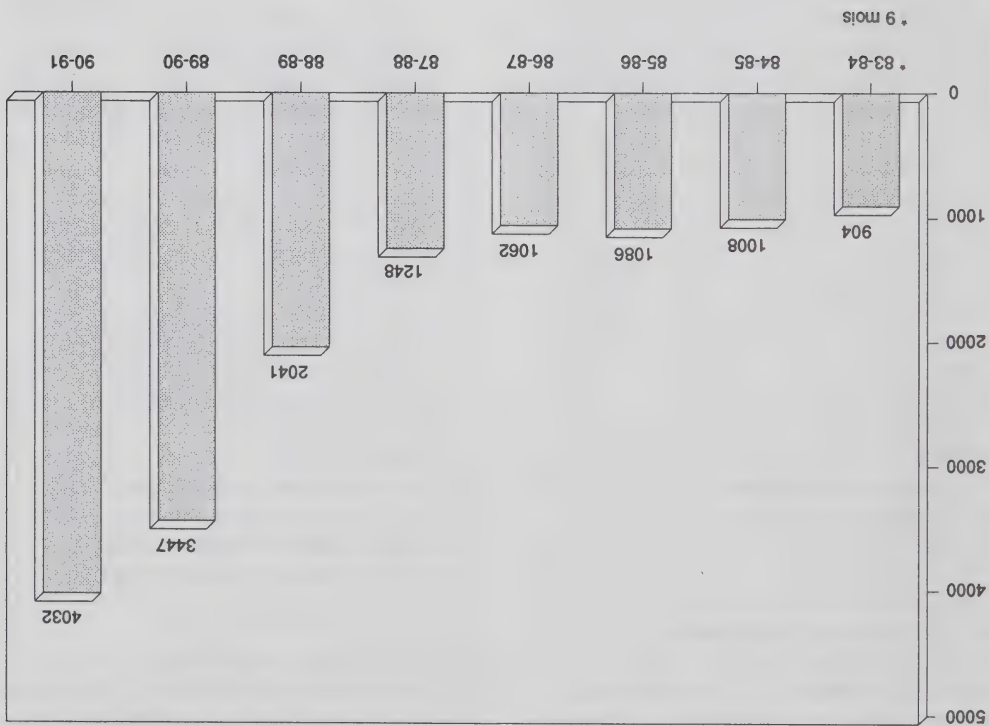
Le nombre de demandes de renseignements adressées au Commissariat continue d'augmenter. Au cours de l'année écoulée, il a reçu 4032 demandes par téléphone et par lettre, comparativement à 3447 l'an dernier, soit une augmentation de 17 p. 100.

La proportion des demandes d'interprétation de la Loi s'est élevée à 55 p. 100. Ces demandes sont très variées : par exemple, des employés de la Société canadienne des postes ont cherché à savoir s'ils étaient tenus de signer une formule de consentement à la divulgation de leurs dossiers médicaux à l'employeur, des détenus ont demandé si les pénitenciers pouvaient ouvrir leur courrier, et le bureau de l'accès à l'information et de la protection des renseignements personnels de Transports Canada a vérifié si la voix de quelqu'un, enregistrée sur bande audio, est considérée comme un renseignement personnel. Toutes ces demandes ont été achevinées au Conseil du Trésor ou au ministère de la Justice, pour interprétation.

La deuxième en importance des catégories des demandes de renseignements (17 p. 100) concerne des problèmes de protection de la vie privée qui ne relèvent pas de la compétence du Commissaire. Par exemple, 4 p. 100 des demandes ont trait à des organismes fédéraux et à des sociétés d'Etat qui ne sont pas assujettis à la Loi. Dans un cas, un agent du Service correctionnel du Canada a été secoué de constater qu'il apparaissait dans une émission télévisée par la Société Radio-Canada. Le caméraman lui aurait dit qu'il ne le filmait pas, mais qu'il ne faisait que régler son objectif. En raison de cette apparition à la télévision, l'intéressé craignait pour sa vie et pour celle d'autres gardes, car ils étaient parfois menacés par des détenus. Malheureusement étant donné que la Société Radio-Canada n'est pas assujettie à la Loi, le Commissariat n'a rien pu faire.

Une bonne partie des autres demandes (13 p. 100) porte sur d'autres paliers de gouvernement, et fréquemment sur le secteur privé. Ainsi, une femme a téléphoné au Commissariat au sujet d'une formule de demande d'emploi qui lui avait été remise par la Banque canadienne impériale de commerce (BIC). Dans cette formule, la Banque lui demandait l'autorisation de faire divulguer des renseignements personnels sur elle par des organismes de crédit et par d'anciens employeurs. La formule contenait même une déclaration attestant que la permission que la signataire donnait s'appliquait à la divulgation de renseignements personnels la concernant au sens du paragraphe 8(2) de la Loi sur la protection des renseignements personnels.

Requêtes 1983-1991



La Commission royale d'enquête sur les nouvelles technologies de reproduction a demandé au Commissaire des commentaires sur les implications pour la protection de la vie privée des nouvelles techniques de reproduction. Le Commissaire compte présenter un document à ce sujet à la Commission royale, une fois que son étude sur les questions génétiques sera terminée. Pour le moment, il est heureux d'avoir été consulté.

Le Commissariat est toujours ravi d'échanger de l'information avec ceux qui s'intéressent à l'avancement de la protection de la vie privée. Comme les demandes de renseignements débordent souvent son mandat, il fait alors office d'ailleur, en trouvant l'information ou en conseillant à l'intéressé de s'adresser à d'autres sources.

C'est ainsi que le personnel chargé de la recherche a répondu à des demandes de renseignements du nouveau Commissaire fédéral à la protection de la vie privée de l'Australie, qui voulait se renseigner sur les lignes directrices applicables à la recherche médicale au Canada, sur l'application de la politique fédérale de couplage de données à des activités destinées à faire respecter les lois, sur les données concernant la sécurité et le renseignement de sécurité et sur l'expérience acquise au Canada en matière de surveillance secrète.

Le Commissaire a d'ailleurs reçu d'autres demandes de renseignements des antipodes. Par exemple, le Comité Nouvelle-Galles du Sud lui a demandé une évaluation globale de la *Loi sur la protection des renseignements personnels* et de l'expérience acquise par le Commissariat. Le Commissaire aux élections de l'Australie a pour sa part demandé des renseignements sur la protection que la loi canadienne accorde aux dénonciateurs (il n'y a aucune) et Telecom Australia a demandé à savoir comment on traite au Canada le service du contrôle des appels et de l'affichage du numéro de téléphone du correspondant et quels sont les codes de conduite des entreprises de télécommunications.

Le Secrétaire de l'Intérieur de Hong Kong, qui faisait des recherches sur la législation en matière de protection des renseignements, a demandé de l'information sur les systèmes d'enregistrement des ordinateurs et sur les licences d'exploitation des banques de données. Ces deux questions font l'objet en Europe de régimes stricts de protection de renseignements; celui qui est prévu par la *British Data Protection Act* est particulièrement strict. Comme la loi canadienne ne prévoit aucune mesure de protection de ce genre, notre correspondant de Hong Kong a dû être aiguillé ailleurs.

Le personnel du Commissariat a aussi fourni à ses homologues provinciaux de l'information de fond sur

- l'expérience acquise au niveau fédéral en matière de couplage de données (Ontario);
- et sur les implications pour la protection de la vie privée et l'appariement des registres de la santé et des services socio-économiques (Québec).

Enfin, le personnel a compilé les documents fédéraux les plus récents sur les applications informatiques des bases de données gouvernementales et mis sur pied des modalités de gestion de la distribution des bases de données des entreprises commerciales, en réponse à une demande du ministère ontarien de la Consommation et du Commerce sur les implications pour la protection de la vie privée des bases de données publiques.

EIC a reconnu que ces deux «pièces» ne suffiraient peut-être pas et a donc étudié d'autres solutions : autorisations des clients de leur numéro de téléphone ou d'un numéro d'identification personnel (NIP) choisi par eux, comme pour les cartes bancaires. La meilleure solution semble être l'utilisation d'un NIP, mais il aurait fallu un an pour y avoir recours, alors que le projet pilote était sur le point d'être lancé en Ontario. Les pressions internes augmentaient, le Conseil du Trésor avait approuvé le projet et le système allait très bientôt faire l'objet d'un appel d'offres; bref, EIC a décidé d'aller de l'avant sans plus attendre.

Le Commissaire a admis qu'EIC était plus en mesure que quiconque de décider comment se servir de cette technologie pour servir le public. Il a toutefois demandé que le projet soit reporté jusqu'à ce que le système soit doté de protections plus sûres, en faisant remarquer qu'EIC risquait de se retrouver dans l'embarras s'il fallait que des renseignements concernant un de ses clients soient divulgués à tort.

Il était malheureusement trop tard; le projet avait déjà gagné London et Peterborough. EIC est d'avis que cette expansion facilitera la mise au point du système à l'échelle nationale, avec une meilleure protection.

Nouveau système de réponse téléphonique aux demandes de renseignements d'EIC

Le Système de réponse vocale automatisée (SRVA) d'EIC continue de soulever des inquiétudes au Commissariat. Il s'agit d'un projet pilote qui permettrait aux usagers du téléphone à clavier d'obtenir par téléphone de l'information d'ordre général sur l'assurance-chômage, voire des renseignements détaillés sur leurs demandes de prestation. Ils pourraient se servir de leur téléphone pour choisir telles ou telles options, et ils s'identifieraient en donnant leur numéro d'assurance sociale et leur date de naissance. Avec le SRVA, les ordinateurs seraient capables de répondre à des milliers d'appels «ordinaires».

Le Commissariat a appris l'existence du système quand une station radio de Québec lui a demandé si cette utilisation du NAS était bien autorisée. Il est certain qu'EIC peut se servir du NAS, qui a été conçu expressément aux fins de l'assurance-chômage. Toutefois, les NAS et les dates de naissance des gens sont des renseignements si répandus que d'autres que les intéressés risquent d'avoir accès au système, si ce sont les deux seules preuves d'identité exigées.

Avec autant d'applications possibles, les cartes seraient utiles pour d'autres ministères et organismes gouvernementaux, voire pour des entreprises privées. EIC pourrait vendre la capacité inutilisée, qui serait employée pour stocker des données ou pour faire des transactions financières. EIC reconnaît que, dans un contexte d'applications multiples, il faudrait distinguer très nettement les fonctions pour éviter toute fusion ou transfert de données d'un programme à l'autre.

Une grande partie du projet en est encore au stade de la conception. EIC estime qu'il lui faudra de trois à quatre ans pour lancer la partie du programme applicable à l'assurance-chômage, trois à quatre ans de plus pour la mettre entièrement en œuvre et dix bonnes années pour que toutes les applications soient opérationnelles. L'ampleur du projet pourrait d'ailleurs nécessiter des modifications de la loi constituant EIC. A cet égard, le Commissariat a proposé que les changements soient axés sur la protection de la carte et de ses applications éventuelles, plutôt que sur les dispositions nécessaires pour en autoriser l'utilisation.

Emploi et Immigration (EIC) est le fer de lance de la technologie des systèmes dans le milieu de travail. Et ce n'est pas surprenant, étant donné qu'EIC sert quelque 3 millions de prestataires de l'assurance-chômage, reçoit environ 40 millions de rapports de demandeurs et répond à plus de 30 millions de demandes de renseignements par année.

Cartes à mémoire

EIC a informé le Commissariat de son intention de lancer un projet pilote de cartes à mémoire qui seraient remises aux clients de l'assurance-chômage. Ces cartes, qui ressemblent beaucoup à des cartes bancaires ou à des cartes de crédit, sont en fait des mini-ordinateurs dotés d'une mémoire de 64 Kb, ce qui les rend aussi puissants que certains des premiers ordinateurs personnels. Les clients qui demandent des prestations en recevraient une, dont ils se serviraient pour signaler leurs périodes de chômage par l'intermédiaire de machines accessibles au public et reliées aux ordinateurs centraux d'EIC, qui détermineraient leur admissibilité, calculeraient leurs prestations et porteraient le montant à leur compte, sur la carte. Les demandeurs pourraient ensuite utiliser leur carte pour retirer de l'argent d'un guichet automatique ou pour faire des achats aux endroits équipés de machines à débit direct.

Le projet pilote devrait commencer en deux endroits à l'automne de 1991. Dans ce contexte, il y a deux risques manifestes pour la vie privée. Le premier, c'est qu'il faut s'assurer que c'est bien la bonne personne qui a accès au système, et le second, qu'on doit prévenir tout couplage des données utilisées pour le système avec d'autres renseignements personnels qui n'y sont pas liés.

Le premier de ces risques semble avoir été évité. En effet, les clients auront accès au système grâce à un numéro d'identification personnel (NIP) de leur choix. De plus, EIC a prévu une protection interne si poussée qu'il la juge impénétrable. La sécurité du système sera d'ailleurs surveillée étroitement durant le projet pilote, et EIC informera le Commissaire des résultats obtenus à cet égard.

Le second danger sera prévenu grâce à une bonne protection contre les couplages indésirables de données. La carte ne pourra pas être utilisée pour d'autres opérations, et les machines utilisées dans les banques et chez les détaillants n'accepteront que les fonds correspondant à la transaction effectuée.

Néanmoins, EIC croit que la carte pourrait avoir jusqu'à huit applications différentes. Par exemple, elle pourrait relier son détenteur à une base de données électroniques de recherche d'emplois contenant des descriptions des emplois disponibles correspondant à sa formation et à son expérience. Elle pourrait aussi être utilisée pour vérifier et payer les indemnités de formation du détenteur et pour l'inscrire à des programmes de formation.

Il semble que les contribuables visés
seront dûment prévenus et qu'on
prendra grand soin de ne pas leur faire
subir de trop grandes difficultés
financières en raison de ce qu'on
déduira de leurs remboursements
d'impôt.

Cela dit, le Commissariat persiste à
croire que ce genre de recouvrement
des dettes des contribuables ne peut se
faire sans modification de la loi. Il ne
suffit pas d'invoquer la *Loi sur la gestion
des finances publiques* ou de dire qu'un
couplage de données de ce genre
constitue une utilisation des
renseignements « compatible » avec les
fins auxquelles ceux-ci ont été recueillis,
ou que leur divulgation est « pour des
raisons d'intérêt public ».

Comme les dossiers de l'ACDI sont classés par projet ou par pays, il est difficile d'y retrouver les nom et adresse des étudiants en question. Pour se faciliter la tâche, l'ACDI se proposait de mettre sur pied un système de repérage fondé sur un couplage de ses fichiers avec ceux des autorisations délivrées aux étudiants par Emploi et Immigration, qui contiennent les renseignements nécessaires. A cette fin, l'ACDI comptait envoyer un fonctionnaire faire des recherches dans les fichiers d'EIC. Bien que le personnel du Commissariat lui ait fait remarquer que rien dans la Loi ne pouvait justifier ce couplage, l'ACDI a soumis une proposition officielle au Commissaire. Au cours des discussions qui ont suivi, le personnel du Commissariat s'est bien rendu compte qu'on n'avait pas dit grand-chose sur la proposition aux fonctionnaires d'EIC, qui n'arrivaient pas non plus à trouver une justification juridique du couplage. Bref, ils n'avaient pas l'intention d'obtempérer à la demande de l'ACDI.

L'ACDI a donc demandé un plus long délai de consultation. Depuis, elle a soumis deux autres propositions. L'analyse du couplage proposé a révélé une anomalie : l'ACDI ne mentionne dans le guide InfoSource aucun fichier de renseignements personnels sur les étudiants et stagiaires. Le Commissariat en a informé le Conseil du Trésor, qui est chargé de veiller à ce que les organismes gouvernementaux respectent la *Loi sur la protection des renseignements personnels*.

Perception des dettes à même les remboursements d'impôt

L'utilisation par l'administration fédérale du NAS pour identifier ceux qui lui doivent de l'argent et pour déduire son dû de leurs remboursements d'impôt est sans doute l'un des plus vieux exemples de couplage de données.

En juin 1990, le Bureau du Contrôleur général a proposé un projet de recherche en vue d'évaluer l'utilité d'un programme de ce genre pour récupérer une partie des millions de dollars de prêts aux étudiants non remboursés. Le Commissariat a accepté qu'on fasse un couplage de données à des fins de recherche, en maintenant toutefois que l'Etat ne devrait pas retenir d'argent sur les remboursements d'impôt des contribuables à moins que la loi ne soit modifiée au préalable.

Le Commissariat voulait aussi qu'on l'assure qu'il n'y aurait pas de déduction à même les remboursements simplement parce que le même nom aurait figuré dans les deux fichiers couplés. En effet, dans les cas de couplage de données, une vérification indépendante s'impose avant que des mesures administratives quelconques soient prises.

Il n'avait pas encore été possible de rapprocher ces points de vue divergents en février 1991, quand le Gouvernement a déposé son budget. Néanmoins, on a fait allusion à cette occasion-là à des changements susceptibles de permettre à l'administration fédérale de récupérer son argent à même les remboursements d'impôt.

Collecte de renseignements par le Service correctionnel du Canada

Le SCC a informé le Commissariat qu'il comptait améliorer ses méthodes de collecte de « renseignements critiques » sur les personnes qui allaient bientôt s'ajouter à la population carcérale. La nécessité de disposer de renseignements de meilleure qualité lui était sautée aux yeux après que deux personnes récemment libérées de pénitenciers fédéraux aient commis des meurtres à Toronto.

Quand un détenu arrive dans un établissement correctionnel, le SCC demande des renseignements à la police, aux tribunaux et à divers organismes carcéraux et services de libérations conditionnelles. Ces sources n'accordent pas toujours une grande priorité aux demandes du SCC, qui risquent par conséquent de ne pas avoir certains renseignements d'importance critique pour déterminer à quel niveau de sécurité le détenu doit être classé ou quelles sont ses possibilités de libération conditionnelle. C'est dans la Région métropolitaine de Toronto que le problème est le plus aigu.

Par conséquent, le SCC se proposait de passer un marché avec d'anciens policiers de Toronto, qui se seraient chargés de recueillir les renseignements nécessaires.

Le Commissariat a étudié les contrats pour s'assurer qu'ils contenaient des dispositions satisfaisantes sur la collecte et l'utilisation des renseignements personnels recueillis par les contractuels, que la procédure de collecte elle-même était conforme à la Loi sur la protection des renseignements personnels, et que les renseignements recueillis seraient tous conservés dans une banque de données et mis à la disposition des personnes concernées. Le SCC a tenu compte de tous ces points.

Répertoire des étudiants étrangers de l'ACDI

Par ailleurs, le Commissariat a souligné que la divulgation de ces renseignements à des organismes provinciaux pourrait nécessiter leur examen par les homologues provinciaux du Commissaire. Il a aussi recommandé qu'on rédige des protocoles d'entente fédérale-provinciale pour régir les éventuels échanges de renseignements.

Le projet de l'Agence canadienne de développement international (ACDI) d'établir un répertoire des étudiants de l'étranger qu'elle subventionne continue à causer des difficultés au Commissariat.

Personne n'est tenu de se prévaloir de ce service, qui découle d'ailleurs du mandat de la CFP. Les participants lui fournissent directement les renseignements demandés et il leur dit comment il compte les utiliser. La CFP constituera une banque réservée aux données recueillies à cette fin.

La TPS et le NAS

L'avis que Revenu Canada a envoyé au Commissariat au sujet du couplage de données rendu nécessaire par la mise en vigueur de la TPS ne s'est pas fait sans accrocs.

Au début de 1990, le ministre du Revenu a informé le Commissaire que la mise en vigueur de la TPS nécessiterait un certain couplage de données et qu'il se servirait des numéros d'assurance sociale des contribuables pour enregistrer et les particuliers, et les entreprises individuelles. Il a assuré le Commissaire que Revenu Canada prenait très au sérieux le droit à la vie privée de ses clients, et il lui a promis une présentation détaillée dans les quelques mois suivants.

En bien, la loi pertinente a été promulguée, le règlement sur le partage de l'information et l'utilisation du NAS a été adopté, et le Commissaire attend toujours la «présentation détaillée» promise. En fait, ce n'est qu'à la fin de 1990 que Revenu Canada a commencé à se pencher sur les implications du couplage des données pour la protection de la vie privée. Le Commissariat l'a pressé de lui fournir des détails, mais sans succès.

Retrait d'un projet de couplage de répertoires des permis de pêche et des permis de conduire des véhicules

Pêches et Océans a abandonné un projet grâce auquel il voulait renforcer sa capacité d'application de la réglementation des pêches en couplant les répertoires des détenteurs de permis de pêche avec ceux des titulaires des permis de conduire des «véhicules» utilisés pour la pêche. Le Ministère a retiré sa proposition quand il est devenu évident que rien dans la Loi ne pouvait justifier le couplage envisagé.

Couplage des dossiers médicaux des immigrants

Santé et Bien-être social Canada a soumis au Commissariat une proposition en vue d'évaluer l'état de santé global des immigrants grâce à un couplage des fichiers de ses services de santé (de l'immigration) avec les fichiers médicaux provinciaux. Le ministère ne voulait extraire de ces fichiers que des données statistiques, et il s'est engagé à ne pas s'en servir à des fins administratives.

En théorie, il n'est pas nécessaire que le Commissaire approuve un couplage comme celui-là, mais le Commissariat sait gré aux responsables de la Santé de l'en avoir informé. En effet, dans ce secteur, les données sont de nature si délicate que leur couplage continue à inquiéter le Commissaire.

Système de sécurité des renseignements d'Agriculture Canada

Agriculture Canada a consulté le Commissariat au sujet de son projet de transférer certains renseignements personnels sur ses fonctionnaires de son système des ressources humaines à un système assurant la sécurité des renseignements.

Le Ministère s'est adressé au Commissariat dès les premières étapes de son projet de couplage d'épuration. (L'épuration sert à vérifier ou mettre à jour une base de données.) Dans sa proposition, il a expliqué pourquoi il estimait le transfert compatible avec les fins auxquelles les renseignements avaient été recueillis. Il comptait agir vite pour modifier les descriptions de la banque de données afin de refléter le changement. Comme Agriculture Canada avait parfaitement respecté la politique, l'examen de sa proposition s'est fait rapidement ... et sans douleur.

Répertoire des balises de localisation individuelles

Le Commissariat a approuvé le projet du ministère des Communications de mettre en place un nouveau système contenant des données sur les détenteurs de « balises de localisation individuelles ». Ces appareils sont de petits émetteurs portatifs dont les campéurs, canotiers et randonneurs se munissent et qu'ils actionnent en cas d'urgence. Leur signal radio facilite la recherche et le sauvetage.

Nouveau service de counselling professionnel pour les cadres

Le Commissariat ne s'est pas non plus fait tirer l'oreille pour approuver la proposition de la Commission de la fonction publique (CCFP) de constituer un répertoire à l'intention de son nouveau service de counselling confidentiel, qui doit aider les cadres à améliorer leurs aptitudes.

Les Communications voulaient constituer un répertoire auquel les intéressés se seraient inscrits volontairement, et qui aurait contenu des renseignements comme leurs nom, adresse, type de véhicule et d'activité (terrestre, maritime ou aérienne), ainsi que le nom du parent à contacter en cas d'urgence. Le répertoire aurait été mis à la disposition du MDN et de la GRC, et il aurait aussi été couplé avec le système conjoint de renseignements utilisés pour la recherche et le sauvetage du MDN et de Transports Canada.

L'inscription au répertoire sera purement volontaire et les renseignements seront utilisés uniquement aux fins pour lesquelles ils auront été recueillis. Les personnes inscrites devront signer une formule de consentement, et elles seront informées de toute divulgation éventuelle. Enfin, toutes les données personnelles contenues dans le répertoire seront stockées dans une nouvelle banque de données personnelles figurant dans le guide InfoSource.

Les membres du comité craignaient que les deux programmes reçoivent des demandes frauduleuses, faute d'une forme quelconque de vérification. Ils ont donc convenus qu'EIC et la Région métropolitaine de Toronto coupleraient leurs données pour éliminer ce risque. Au début, EIC a déclaré que le couplage était « compatible » avec les fins auxquelles les renseignements avaient été recueillis, sans donner guère plus d'explications au Commissaire. Toutefois, après de longues consultations, les responsables ont donné la raison d'être du couplage et fourni des arguments juridiques pour le justifier.

Le Commissaire s'est dit satisfait, mais il a demandé à EIC de suivre l'exemple de la Région métropolitaine de Toronto, en disant aux demandeurs que leur admissibilité devait être vérifiée par les autorités. Il lui a en outre demandé d'ajouter un avis et une déclaration de consentement à ses formules de demande, ainsi que de vérifier si le couplage réduisait suffisamment le nombre de demandes frauduleuses pour en valoir la peine. EIC a accepté.

Le projet INFONNEL des Affaires extérieures

Dans le rapport annuel de l'an dernier, nous avions dit que les Affaires extérieures avaient demandé au Commissariat d'étudier le système de gestion du personnel dont elles envisageaient de se doter, et qui aurait consisté à fusionner de petites bases de données pour en faire un système intégré offrant des possibilités de traitement plus étendues. Le système devait permettre à la direction de prévoir, suivre et enregistrer toutes les mesures prises dans le domaine du personnel.

Le personnel du Commissariat craignait que les applications rendues possibles par le degré d'intégration envisagé excèdent les limites approuvées par le Conseil du Trésor pour ce genre de base de données; de plus, la proposition ne contenait pas suffisamment de détails sur les caractéristiques de sécurité du système. Bref, sa conception ne satisfaisait pas aux exigences de la *Loi sur la protection des renseignements personnels* ou de la politique de sécurité gouvernementale.

Les difficultés n'ont pas pu être résolues grâce aux documents de suivi et aux discussions qui ont eu lieu par la suite, de sorte que les vérificateurs du Commissariat devront analyser le système.

Couplage de données informatiques

Le traitement électronique des données présente des risques particuliers pour la vie privée. Ainsi, le couplage incontrôlé de fichiers informatiques pourrait aboutir à la production de dossiers détaillés sur tout le monde, ce qui tournerait en ridicule les restrictions imposées par la Loi en matière de collecte des renseignements.

Pour parer à ce risque, l'administration fédérale s'est donnée il y a un peu plus d'un an une politique de couplage des données obligeant les ministères et organismes à soumettre au Commissaire à la protection de la vie privée des propositions détaillées au moins 60 jours avant de commencer à établir une liaison entre bases de données. La politique freinera le couplage incontrôlé des données en permettant à un tiers, le Commissaire à la vie privée, d'évaluer leurs propositions en toute indépendance, à partir d'un ensemble de critères dûment approuvés. Le Commissaire jouera aussi le rôle de défenseur de tous ceux qui pourraient être affectés par les résultats.

Malheureusement, certains ministères et organismes semblent avoir l'impression que le Commissaire doit simplement se contenter d'approuver leurs projets après en avoir été informé à la dernière minute. La politique du Conseil du Trésor est pourtant claire, et le Commissaire fait ses évaluations avec sérieux. Ceux qui le préviennent quand leur système est déjà prêt à démarrer ne feront que causer des retards frustrants pour tous les intéressés.

Cette année, le personnel du Commissariat a étudié 11 propositions soumises en vertu de la politique. Dans les pages qui suivent, nous allons donner une description succincte de chacune d'entre elles, avec un résumé de nos conclusions. Pour obtenir plus de détails - ou des conseils sur la façon de préparer des propositions - il suffit de nous téléphoner.

Couplage des fichiers du Programme d'aide à l'adaptation d'Emploi et Immigration Canada avec ceux du bien-être social de la Région métropolitaine de Toronto

Des représentants des autorités fédérales et ontariennes ainsi que de la Région métropolitaine de Toronto ont formé un comité pour résoudre certains des problèmes résultant du nombre croissant de personnes de cette Région qui ont réclame le statut de réfugié et qui touchent des prestations de bien-être social.

Il s'agit notamment de savoir si ces gens reçoivent une aide financière du Programme d'aide à l'adaptation d'Emploi et Immigration Canada, qui donne de l'argent aux réfugiés jusqu'à ce que ceux-ci aient des revenus suffisants pour subvenir à leurs besoins (ou pour une période d'un an, selon la première des deux éventualités). Les réfugiés qui bénéficient de l'aide financière du Programme ne peuvent pas toucher de prestations de bien-être social.

Fournir des détails pareils va au-delà des exigences de l'imputabilité. Après avoir fait cette erreur, le CRDI ne pouvait plus refuser de divulguer les noms des intéressés. Le Commissaire a donc accepté qu'il le fasse, comme il l'en avait avisé, et le CRDI a informé les membres de son conseil d'administration de la divulgation.

Un piètre coup de filet pour Revenu Canada

Pêches et Océans Canada a avisé le Commissaire de son intention de fournir au Bureau des communications (TPS) de Revenu Canada une liste d'adresses postales de pêcheurs commerciaux. Le Bureau de la TPS voulait envoyer à ces pêcheurs une brochure d'information leur expliquant comment facturer, consigner, calculer et verser la taxe. Revenu Canada n'avait pas d'autres moyens de communiquer avec les pêcheurs, de sorte que Pêches et Océans a conclu qu'il était manifestement à l'avantage de ces derniers de recevoir le document en question. Le Commissaire n'en était pas si sûr. En effet, la loi portant création de la TPS n'avait pas encore été adoptée, et, bien que la divulgation de la liste aurait pu être utile, il n'était pas convaincu qu'elle allait présenter un avantage certain pour les pêcheurs. Néanmoins, il a déclaré à Pêches et Océans qu'il ne s'opposait pas à son envoi de la brochure pour le compte de Revenu Canada.

Pêches et Océans n'a pas jugé avoir des raisons d'intérêt public suffisantes pour se charger de l'envoi postal de la brochure sur la TPS, en décidant toutefois de fournir à Revenu Canada une liste des associations de pêcheurs.

Les noms des membres du conseil d'administration ne sont pas des renseignements «personnels»

Le Centre de recherches pour le développement international (CRDI) a informé le Commissaire qu'il divulguerait les noms des membres de son conseil d'administration qui avaient assisté à une de ses réunions, à Bangkok, en Thaïlande. Le Centre avait donné à un journaliste (qui en avait fait la demande en vertu de la Loi sur l'accès à l'information) un relevé des notes de frais de ces personnes, mais pas leurs noms. Le journaliste s'était plaint au Commissaire à l'information, qui avait recommandé au CRDI de divulguer les renseignements demandés.

Après avoir discuté de l'avis qu'il avait reçu avec le personnel du CRDI, le Commissaire à la protection de la vie privée a souscrit au raisonnement du Commissaire à l'information, qui estimait que les membres du Conseil d'administration du Centre faisaient partie de son personnel de direction et que, par conséquent, leurs notes de frais ne seraient pas normalement considérées comme des «renseignements personnels». Toutefois, en préparant les documents réclamés par le journaliste, le CRDI avait fait figurer plus de détails que nécessaire (les plats commandés, les numéros d'assurance sociale et le genre de cartes de crédit des membres, voire le numéro de carte American Express de l'un d'eux).

Le MDN était en proie à un dilemme en ce qu'il avait accepté de traiter confidentiellement des renseignements qui semblaient contredire les accusations portées contre l'intéressé par l'ancienne fonctionnaire. Comme l'intéressé ne savait peut-être pas que ces renseignements figureraient dans son dossier, il aurait pu être privé de détails d'une importance cruciale pour sa défense. Le MDN a conclu qu'il était nécessaire, pour des raisons d'intérêt public, de lui fournir ces renseignements avant le début du procès.

Le Commissaire a informé l'ancienne fonctionnaire de la divulgation.

Une femme reçoit des détails sur les circonstances entourant le décès de son fils à l'étranger

Une femme a demandé à la GRC et aux Affaires extérieures de lui communiquer les renseignements qu'elles détenaient sur les circonstances entourant le décès de son fils en Thaïlande. La GRC et les Affaires extérieures estimaient que l'enquête menée par les autorités thaïlandaises avait été concluante, et un pathologiste canadien avait confirmé les résultats de l'autopsie pratiquée sur place, mais la mère se posait encore des questions, de sorte que la GRC voulait lui communiquer 21 des pages de son rapport d'enquête, en n'en retirant que quelques renseignements concernant d'autres personnes. Pour leur part, les Affaires extérieures étaient disposées à lui fournir des documents tirés des dossiers conservés dans deux de ses ambassades à l'étranger ainsi qu'à son administration centrale, à Ottawa.

Normalement, la Loi sur la protection des renseignements personnels interdirait la divulgation de ces renseignements, même à la mère du défunt. Toutefois, les deux organismes en cause jugeaient qu'il était préférable, pour des raisons d'intérêt public, de lui communiquer le rapport afin qu'elle puisse poursuivre ses démarches en Thaïlande, et afin aussi de la rassurer, si possible. Le Commissaire s'est dit d'accord.

Un demandeur cherchait à obtenir une liste de dividendes non réclamés

Un demandeur a invoqué la Loi sur l'accès à l'information pour obtenir de Consommateurs et Sociétés Canada (CSC) des listes de dividendes non réclamés en vertu de trois lois, la Loi sur la faillite, la Loi sur les sociétés par actions et la Loi sur les liquidations. Il voulait retracer les créanciers.

CSC a avisé le Commissaire de son intention de divulguer les listes demandées, parce que ce serait à l'avantage des individus concernés (sous-aligné 8(2)(iii)). Le Commissaire s'est dit d'accord, mais en ajoutant qu'il ne cessait pas d'éprouver un certain malaise quant à l'opportunité d'une telle divulgation. Il a souligné que, si les institutions gouvernementales sont capables de retracer sans trop de mal les personnes auxquelles elles doivent de l'argent, ne lui semblait vraiment pas idéal de divulguer des renseignements personnels sans le consentement des intéressés, pour permettre à des tiers de localiser des créanciers, sans doute moyennant rétribution.

Cette année, le Commissariat a reçu 50 préavis d'organismes gouvernementaux qui allaient divulguer des renseignements personnels pour des raisons « d'intérêt public » ou à l'avantage des personnes concernées. Ces divulgations allaient de la confirmation de la citoyenneté des intéressés, afin que ceux-ci puissent toucher des pensions ou des indemnités, jusqu'à des rapports détaillés sur des évasions de pénitenciers fédéraux. En fait, les incidents impliquant des détenus sont désormais une constante dans les cas de préavis (voir la page 28 pour plus de détails).

Voici quelques exemples d'autres préavis pour des raisons d'intérêt public.

Le MDN divulgue des détails tirés d'un dossier d'attestation de sécurité

Le ministère de la Défense nationale (MDN) a avisé le Commissaire de son intention de divulguer à un fonctionnaire des renseignements normalement jugés confidentiels, tirés de son dossier d'attestation de sécurité.

Le personnel du MDN était en train d'étudier la demande que l'intéressé avait présentée pour voir son dossier lorsqu'il a appris que la sûreté provinciale avait porté des accusations de nature criminelle contre lui, notamment dans un cas d'agression sexuelle contre une ancienne fonctionnaire. Le dossier d'attestation de sécurité du demandeur contenait un compte rendu de l'interrogatoire auquel la fonctionnaire plaignante avait été soumise par la police militaire, et durant lequel elle avait donné des détails sur sa longue liaison sexuelle avec l'intéressé. Elle avait fait clairement comprendre à la police militaire que cette liaison était désirée par les deux parties.

Comme la Loi sur la protection des renseignements personnels autorise les organismes d'enquête (y compris la police militaire) à protéger les sources interrogées au cours des enquêtes effectuées en vue d'accorder des attestations de sécurité, le MDN aurait normalement refusé de divulguer les commentaires de la fonctionnaire en question, car ils la concernaient tout autant que l'intéressé, et il aurait été virtuellement impossible de ne tirer du dossier que les renseignements concernant ce dernier; en outre, la source des renseignements aurait été évidente.

Toutefois, il était clair que Transports Canada avait compilé la liste de certains des participants à l'enquête à partir de renseignements personnels recueillis à d'autres fins, dont aucune ne comprenait leur divulgation à des organismes de recherche. Dans la plupart des secteurs, Transports Canada n'avait donné à l'entreprise chargée de l'enquête que le nom et le numéro de téléphone des participants éventuels, mais, dans le cas du personnel aéroportuaire, on avait utilisé une liste d'employés titulaires de permis de conduire des véhicules côté piste; comme la divulgation de leurs noms n'était pas compatible avec les fins auxquelles ils avaient été recueillis, elle n'était pas justifiée.

L'agent enquêteur a aussi constaté que les responsables de l'enquête avaient commencé à recueillir des renseignements avant même d'avoir signé des contrats écrits. Or, les projets de contrats étaient muets sur les principes de collecte de renseignements prévus par la Loi. Par conséquent, des représentants du Commissariat, d'Approvisionnement et Services

(l'organisme qui passait les marchés d'enquête) et de Transports Canada se sont réunis pour fixer des règles ayant pour objet d'assurer que tous les marchés conclus à des fins de collecte de renseignements personnels contiendront des clauses normalisées sur la collecte, la conservation, l'utilisation, la divulgation et le retrait de ces renseignements, de façon à être conformes à la Loi.

Le Commissaire a par ailleurs recommandé à Transports Canada d'obtenir le consentement des personnes visées avant d'envisager toute utilisation ultérieure des renseignements personnels les concernant qui ne serait pas compatible avec les fins auxquelles ceux-ci auraient été recueillis à l'origine.

La liste des titulaires de permis ne doit pas être utilisée pour des enquêtes

Lorsqu'un dirigeant d'une compagnie aérienne a téléphoné au Commissariat au sujet d'une enquête de Transports Canada sur l'utilisation de médicaments et de drogues, le Commissaire a décidé d'enquêter de sa propre initiative.

Le correspondant du Commissaire avait commencé à s'inquiéter quand une entreprise de recherche sur les marchés lui avait demandé le nom, l'adresse et le numéro de téléphone de ses employés. L'entreprise en question lui avait dit qu'elle avait été chargée par Transports Canada d'une enquête sur l'utilisation de médicaments, de drogues et d'autres substances dans le secteur des transports, et qu'elle avait besoin de ces renseignements personnels pour choisir au hasard les personnes qui allaient participer à l'enquête.

Il s'est avéré que l'enquête en question était un important volet de l'étude que Transports Canada avait amorcée en vue de déterminer dans quelle mesure la consommation de médicaments, de drogues et d'alcool par les employés du secteur des transports représentait un danger pour la sécurité dans ce domaine. Les répondants devaient remplir un questionnaire sur leur consommation d'alcool, de médicaments (sur ordonnance et en vente libre), de drogues, de même que sur les conditions existant à leur lieu de travail qui pouvaient influencer sur leur utilisation de ces substances.

À cet égard, il fallait se poser deux questions en ce qui concerne la protection de la vie privée, à savoir si les règles de collecte des renseignements personnels avaient été respectées pendant l'enquête, et si Transports Canada avait respecté les dispositions sur l'utilisation et la divulgation de ces renseignements prévues par la Loi sur la protection des renseignements personnels.

Ces restrictions en matière d'utilisation et de divulgation obligent les ministères et organismes fédéraux à recueillir seulement les renseignements personnels ayant un lien direct avec leurs programmes ou leurs activités. En outre, ces renseignements doivent être recueillis directement auprès de la personne intéressée, chaque fois que possible, à moins que cela n'amène les responsables à recueillir des renseignements incorrects, contraire les fins auxquelles ceux-ci sont destinés ou en compromette l'usage. En outre, la personne intéressée doit être informée des fins auxquelles les renseignements recueillis sont destinés.

L'enquête a révélé que les questionnaires ne contenaient pas de renseignements personnels permettant de les relier à quelqu'un de précis. Bref, étant donné que les répondants ne pouvaient pas être identifiés, les renseignements recueillis n'étaient pas véritablement «personnels», de sorte que leur collecte ne constituait pas une infraction à la Loi sur la protection des renseignements personnels.

Il n'empêche que le Règlement est clair. Le Commissaire a conclu que la CRTFP doit conserver les pièces contenant des renseignements personnels au moins deux ans après la dernière mesure administrative prise à leur égard. La Commission a accepté cette conclusion, et le Commissaire a jugé la plainte résolue.

Les renseignements personnels divulgués devraient être corrects

Un employé de longue date de la Société canadienne des postes (SCP) s'est plaint au Commissaire que son employeur avait communiqué des renseignements médicaux incorrects à son sujet à la Commission des accidents du travail, afin de lui faire refuser des prestations auxquelles il avait droit.

La SCP avait déclaré à la Commission des accidents du travail que le plaignant n'avait pas droit à ces prestations parce que sa blessure était imputable à des troubles chroniques. La superviseuse du plaignant a déclaré que c'était le plaignant lui-même qui lui avait déclaré cela, et qu'elle n'avait fait que répéter des faits qu'elle croyait pertinents dans le contexte de sa réclamation.

Pour sa part, le plaignant a nié souffrir de troubles chroniques, et ses dires ont été confirmés lorsqu'il s'est fait examiner par un spécialiste. Il a aussi nié avoir jamais dit à quiconque, et surtout pas à sa superviseuse, qu'il souffrait d'une affection de ce genre.

L'agent enquêteur a constaté un facteur qui peut avoir envenimé la situation. En effet, la SCP ne lâche pas facilement le morceau dans le contexte des accidents du travail, dans le but de limiter les frais le plus possible. Elle prétend d'ailleurs être tenue de divulguer à la Commission des accidents du travail tout renseignement susceptible de mettre en doute la validité des réclamations.

La Loi sur la protection des renseignements personnels dispose

que les renseignements de cette nature utilisés à des fins administratives doivent être aussi exacts, à jour et aussi complets que possible. Dans ce cas-ci, rien ne permet de croire que la superviseuse ait fait le moindre effort pour vérifier la validité des renseignements médicaux qu'elle avait communiqués à la Commission des accidents du travail.

Après avoir longtemps discuté, la SCP a fini par accepter de déclarer à la Commission des accidents du travail qu'elle n'avait aucune preuve de sa prétention que le plaignant souffrait des troubles en question.

Le Commissaire a jugé la plainte bien fondée et résolue.

La Commission des relations de travail dans la fonction publique conserve désormais ses pièces pendant deux ans

Bien que le Règlement sur la protection des renseignements personnels oblige les organismes gouvernementaux à les conserver au moins deux ans, une plainte a révélé que la Commission des relations de travail dans la fonction publique (CRTFP) ne conservait ses pièces que trois mois avant de les faire détruire ou de les renvoyer à la partie qui les avait déposées.

Le Règlement prévoit une période de conservation de deux ans pour que les citoyens aient l'occasion de consulter les documents qui les intéressent. Une femme s'est plainte qu'on avait porté atteinte à ses droits de protection des renseignements personnels parce que la CRTFP avait détruit des pièces bien avant l'expiration de la période de deux ans.

La CRTFP a expliqué à l'agent

pièces, qui peuvent comprendre aussi bien des volumes entiers de documents que des articles aussi hétéroclites qu'un bâton de baseball brisé, des poubelles, voire une corde de pendu! La Commission a de plus souligné que toutes les parties aux audiences reçoivent copie des pièces, de sorte que rien n'est détruit qu'elles n'aient déjà reçu.

Le personnel du Commissariat a eu plusieurs rencontres avec des représentants du Conseil du Trésor, qui ont déclaré que la participation au régime de dépôt direct était encore volontaire, et que Transports Canada avait tout simplement été trop pressé de commencer. On n'avait recueilli des renseignements qu'après des personnes qui avaient décidé d'adhérer au régime. Cela dit, l'employeur était conscient du problème qu'allait poser les récalcitrants.

Néanmoins, compte tenu de ce que le Président du Conseil du Trésor avait annoncé en décembre 1989, il semblait bien que la fonction publique s'orientait vers un régime de dépôt direct obligatoire. Le Commissaire a donc décidé de garder le dossier ouvert jusqu'à ce que la politique soit plus claire.

Le 15 décembre 1990, l'employeur a annoncé que la participation au régime de dépôt direct demeurerait volontaire. Les plaignants ne seraient pas tenus de divulguer l'information nécessaire, et l'employeur n'ouvrirait pas de compte en leur nom. Le Commissaire a conclu que la plainte n'était pas fondée.

Le plaignant avait déclaré que cette

situation n'équivalait pas à une

condamnation au pénal dans l'État en

question. L'agent d'immigration a alors

écrit au Greffier de la Première Cour de

circuit de l'État pour obtenir son opinion

à ce sujet. Ce faisant, il a divulgué le

fait que le plaignant avait demandé le

statut de réfugié au Canada. La Cour

de l'État a confirmé que la déclaration

de culpabilité équivalait à une

condamnation.

Comme l'un des objectifs de la *Loi sur*

l'immigration est de promouvoir l'ordre

et la justice à l'échelle internationale, en

n'acceptant pas sur le territoire

canadien des personnes susceptibles

de se livrer à des activités criminelles, le

Commissionnaire a décidé qu'il s'agissait

d'une utilisation des renseignements

compatible avec les fins auxquelles

ceux-ci avaient été recueillis, et que, par

conséquent, le geste de l'agent

d'immigration était justifié. Il a donc

décidé que la plainte était non fondée.

Une demande de renseignements prématurée : l'affaire du dépôt direct

Quand l'administration fédérale a

annoncé qu'elle cesserait de payer les

fonctionnaires par chèque à partir du

1^{er} avril 1991 et qu'elle commencerait

alors à déposer le montant

correspondant directement dans leur

compte bancaire, plusieurs

fonctionnaires ont communiqué avec le

Commissionariat pour savoir s'ils étaient

tenus de divulguer leur numéro de

compte à l'employeur.

consentement?

ouvrir un compte sans leur

banque, en demandant à celle-ci de leur

numéro d'assurance sociale à une

donner leur nom, leur adresse et leur

fournir ces renseignements. Allait-il

fonctionnaires qui refuseraient de lui

l'employeur allait réagir dans le cas des

Il restait encore à savoir comment

administrer la paye.

recueillant l'information qu'il lui faut pour

renseignements personnels en

violerait pas la *Loi sur la protection des*

fonctionnaires. Par conséquent, il ne

décider comment payer ses

l'employeur a effectivement le droit de

Le Commissionnaire a conclu que

renseignements?

Loi l'autorise-t-elle à recueillir ces

bancaire aux fins du dépôt direct? La

succursale et le numéro de leur compte

fonctionnaires à leur indiquer leur

l'employeur, peut-il obliger les

Le Conseil du Trésor, autrement dit

Ministère. Il n'était vraiment pas

demandar ce renseignement par le

Transports Canada, qui s'était fait

due forme d'un fonctionnaire de

a été saisi d'une plainte en bonne et

Le Commissionnaire a fait enquête lorsqu'il

Le Commissaire a analysé la politique de perception de Revenu Canada, et il a reconnu que l'agent de perception avait besoin d'examiner les dépenses personnelles de la contribuable. Par conséquent, celle-ci était tenue par la Loi de l'impôt sur le revenu de fournir ce genre de renseignements. Le Commissaire a donc jugé que Revenu Canada avait respecté les dispositions sur la collecte de renseignements de la Loi sur la protection des renseignements personnels et conclu que la plainte n'était pas fondée.

La politique d'embauche doit concilier l'équité et le droit à la vie privée

Conformément à la politique sur les appels de la Commission de la fonction publique, les ministères et organismes ne sont tenus de divulguer que les renseignements personnels directement pertinents concernant les candidats sélectionnés. En l'occurrence, on s'était servi des évaluations de rendement pendant la procédure de dotation, mais elles n'avaient pas été mentionnées pendant l'appel et il n'en avait pas été tenu compte dans la décision d'appel. Elles n'étaient donc pas pertinentes. Leur divulgation a entraîné une grave violation du droit à la vie privée des plaignants, même si, au départ, l'agent de dotation a peut-être simplement déché par souci exagéré d'équité.

EIC a rappelé à toutes ses divisions du personnel la politique de divulgation des renseignements de ce genre. En outre, elle distribuera des lignes directrices plus détaillées pour faciliter le travail des agents de dotation, pris entre l'encumbe de l'équité dans leur travail et le marteau de la protection de la vie privée des candidats.

Divulgateion au pays d'origine d'une demande de statut de réfugié

Le plaignant, qui avait demandé le statut de réfugié, a reproché à un agent d'Emploi et Immigration Canada d'avoir communiqué des renseignements personnels à son sujet aux Etats-unis sans son autorisation.

Au cours de l'audition de sa demande de statut de réfugié, on avait constaté que le plaignant avait été déclaré coupable d'une infraction criminelle alors qu'il se trouvait aux Etats-Unis, mais qu'il ne s'était pas présenté pour se faire imposer sa peine.

Deux candidates qui avaient gagné un concours interne d'EIC ont porté plainte au Commissariat en disant qu'une agente de dotation avait communiqué leurs évaluations de rendement et les noms des personnes qui devaient leur fournir des références à une autre fonctionnaire qui en appelait des résultats du concours. Cette fonctionnaire avait par la suite divulgué le tout à l'ensemble du personnel du bureau des deux candidates sélectionnées.

Revenu Canada peut avoir accès aux relevés des dépenses personnelles des contribuables

Une Ontarienne qui avait des difficultés à payer ses arrearages d'impôt fédéral a porté plainte contre Revenu Canada (impôt). Elle s'est fâchée quand un agent du fisc a insisté pour examiner ses dépenses personnelles afin d'évaluer sa capacité de payer, en invoquant la Loi de l'impôt sur le revenu. La contribuable jugeait que le procédé était abusif et qu'il violait sa vie privée.

L'article 4 de la *Loi sur la protection des renseignements personnels* dispose que : « Les seuls renseignements personnels que peut recueillir une institution fédérale sont ceux qui ont un lien direct avec ses programmes ou ses activités. » Par conséquent, les fonctionnaires fédéraux ne peuvent recueillir que les renseignements personnels dont ils ont manifestement besoin pour administrer leurs programmes.

Revenu Canada a expliqué qu'il est chargé de percevoir l'impôt sur le revenu des particuliers aux fins de l'application de la *Loi de l'impôt sur le revenu*. Sa procédure de perception est conçue de façon que cette Loi s'applique également à tous les contribuables, tout en lui permettant de tenir compte de la situation financière de chacun. Pour être juste avec la majorité des citoyens, qui payent sans tarder, la politique est ferme à l'endroit de ceux qui se font tirer l'oreille.

La CCDF avait refusé de divulguer à la plaignante les adresses et numéros de téléphone d'autres personnes, ainsi que les déclarations des témoins. Le Commissaire a reconnu que la CCDF avait eu raison de refuser de divulguer les renseignements personnels concernant des tiers, mais il a contesté la non-divulgence des témoignages une fois l'enquête terminée.

En général, le Commissaire est d'avis que les témoignages ne devraient pas être divulgués tant que l'enquête est en cours, étant donné que leur divulgation risquerait d'influer sur ses résultats. En l'occurrence, toutefois, l'enquête était déjà terminée. Le Commissaire a donc demandé à la CCDF ce qu'on risquait si la plaignante était autorisée à consulter les témoignages.

La CCDF a été incapable de prouver que la divulgation des témoignages risquait vraiment de nuire à l'enquête en question ou à des enquêtes ultérieures. Néanmoins, le Commissaire a dû beaucoup insister avant qu'elle finisse par accepter de divulguer les témoignages à la plaignante.

Comme les renseignements demandés avaient d'abord été refusés, le Commissaire a jugé la plainte bien fondée, mais résolue.

Il n'est pas possible de refuser de divulguer des renseignements à un demandeur s'ils doivent être communiqués à son médecin

Un ancien militaire a porté plainte au Commissaire quand les Archives nationales ont refusé de lui communiquer certaines parties de ses dossiers médicaux datant de l'époque où il était militaire, en invoquant l'article 28 de la Loi pour dire que l'examen d'une évaluation de son état de santé mentale faite 25 ans auparavant le desservirait. Par contre, les Archives écrites, à divulguer les renseignements demandés à son médecin, qui aurait pu lui expliquer l'évaluation en question.

Le plaignant soutenait qu'il connaissait la teneur de son évaluation et qu'il n'avait pas besoin d'explications. Le Commissaire a jugé que, si les Archives étaient d'avis qu'il serait à l'avantage du demandeur de ne pas voir le dossier en question, elles auraient dû refuser catégoriquement de le divulguer. Par contre, si elles étaient disposées à le divulguer, même par l'intermédiaire de son médecin, il était illogique qu'elles prétendent que sa divulgation allait desservir le plaignant.

Les témoignages doivent être divulgués à la fin des enquêtes

Le Commissaire s'est aussi demandé pourquoi les Archives voulaient refuser de communiquer le dossier au plaignant en se fondant sur l'évaluation qu'un psychiatre retenu à cette fin avait faite du dossier quand le plaignant avait présenté des demandes analogues, en 1985 et en 1990. Le Commissaire a conclu que cette évaluation psychiatrique n'était pas digne de foi, étant donné qu'elle n'était fondée que sur un examen de dossiers médicaux datant de 25 ans et qu'elle ne tenait pas compte de l'état émotionnel actuel du plaignant.

Les renseignements réclamés ont été divulgués après que le Commissaire eut conclu que le plaignant avait le droit de voir son dossier. Qui plus est, les Archives nationales ont accepté de modifier leur procédure de traitement des renseignements médicaux de nature délicate. À l'avenir, elles refuseront tout simplement de divulguer ces renseignements, ou les divulgueront directement au demandeur ou à son médecin.

Une dame qui avait porté plainte à la Commission canadienne des droits de la personne (CCDP) dans un cas de discrimination avait demandé à voir les renseignements contenus dans son dossier de plainte. Quand la CCPD a refusé de lui communiquer certains de ces renseignements, elle s'est plainte au Commissaire à la protection de la vie privée.

Les militaires doivent avoir plus facilement accès à l'information lorsqu'ils présentent des griefs

Une plainte portée contre le ministère de la Défense nationale (MDN) n'a peut-être incité à modifier sa procédure de règlement des griefs des militaires. L'affaire a soulevé d'importantes questions sur l'accès des militaires aux renseignements factuels recueillis dans ce contexte par le service du contentieux du MDN.

Les avocats du MDN peuvent faire enquête sur les griefs des militaires afin de préparer des avis juridiques et de conseiller le chef de l'État-major de la Défense. Dans l'administration fédérale, ce sont normalement des agents des relations de travail (qui ne sont pas avocats) qui font enquête sur les griefs. La procédure utilisée dans le cas des militaires fait qu'une proportion accrue des documents pertinents est protégée par le secret professionnel qui lie l'avocat à son client.

Les problèmes que cela cause ont sauté aux yeux du Commissaire quand un officier s'est plaint que le MDN lui avait refusé une grande partie des renseignements contenus dans son dossier de grief en invoquant le secret professionnel ou en disant qu'il s'agissait de renseignements personnels concernant des tiers. L'agent enquêteur a confirmé que le MDN s'était réclamé de la relation privilégiée entre l'avocat et son client pour tous les documents obtenus ou rédigés par son service du contentieux

commandement.

pendant l'enquête sur le grief. Le MDN a soutenu que les documents devaient être protégés puisque ses avocats avaient préparé le dossier dans le but exprès de rédiger un avis juridique et des recommandations pour le haut commandement. Le Commissaire a contesté une interprétation aussi large du secret professionnel qui lie l'avocat à son client, en déclarant à la fois injuste et contraire à l'intention du législateur qu'on invoque cette protection pour éviter de communiquer des faits et des témoignages recueillis au cours de l'enquête. Il a proposé au MDN de se prevaloir de sa latitude pour communiquer plus de renseignements au plaignant. Le MDN a accepté de réévaluer sa position; l'officier a reçu 10 autres pages de texte, comprenant notamment les déclarations des témoins.

Par ailleurs, le Commissaire a admis que le reste des documents qui n'avaient pas été communiqués au plaignant contenait des renseignements personnels sur des tiers, et que le MDN avait donc eu raison de ne pas les divulguer. Depuis, le MDN a révisé sa procédure de règlement des griefs des militaires, et communiqué désormais à ceux-ci tous les documents (à quelques rares exceptions près) dont il doit être tenu compte à l'arbitrage de leurs griefs.

Revenu Canada n'a pas pu expliquer pourquoi il n'avait pas accusé réception de la demande de la plaignante, pourquoi il ne lui avait pas dit quand lui fournirait le dossier et, en fin de compte, pourquoi il n'a pas respecté le délai.

Le Commissaire a jugé la plainte bien fondée.

La Cour fédérale ordonne au SCRS de répondre

Le Service canadien du renseignement de sécurité (SCRS) a informé un demandeur qu'il ne pouvait pas lui fournir les renseignements personnels que celui-ci réclamait dans les 30 jours prévus par la Loi.

demandes.

Le demandeur a porté plainte au Commissaire et déclaré à l'agent enquêteur qu'il s'adresserait à la Cour fédérale si le SCRS ne lui donnait pas les renseignements dans le délai maximum de 60 jours autorisé par la Loi.

Le 6^e jour, après avoir constaté que le SCRS n'avait toujours pas fini de traiter les dossiers du plaignant, le Commissaire conclut que la plainte était bien fondée, et il lui a confirmé son droit de saisir la Cour fédérale de l'affaire. (Les plaignants ne peuvent pas se prévaloir de leur droit de recours en révision devant la Cour fédérale tant que l'enquête du Commissaire n'est pas terminée.)

Le plaignant a demandé à la Cour de délivrer un mandamus enjoignant au SCRS de produire les renseignements qu'il réclamait. Sa requête a été entendue 20 jours plus tard, et le juge a ordonné au SCRS de donner réponse à la demande du plaignant dans un délai d'un mois à partir de la date du jugement. Le SCRS a obtempéré.

Bien que le SCRS ait fini par produire les renseignements réclamés, l'audience et le délai supplémentaire d'un mois que la Cour lui a accordé ont prolongé de 50 jours la période d'attente du plaignant. La solution n'est vraiment pas satisfaisante; huit ans après la promulgation de la *Loi sur la protection des renseignements personnels*, il est inacceptable que les demandeurs doivent s'adresser à la Cour fédérale pour forcer une institution fédérale à leur communiquer les renseignements qu'ils réclament dans les délais prévus par la Loi.

Les dossiers de l'impôt ne doivent pas être utilisés par des admirateurs

Une journaliste a reçu à son domicile une lettre d'un admirateur qui est fonctionnaire fédéral. Elle a téléphoné au Commissariat pour savoir comment l'intéressé avait pu trouver son adresse personnelle. Elle ne voulait pas porter plainte, ni causer des difficultés à son admirateur, mais elle tenait à assurer sa sécurité et désirait savoir comment celui-ci s'était procuré son adresse.

Le Commissariat a eu beaucoup de mal à respecter les désirs de la journaliste tout en prenant des mesures pour que les fonctionnaires fédéraux évitent d'utiliser les dossiers gouvernementaux à des fins qu'on ne peut vraiment pas juger « compatibles » avec leurs fonctions, même avec la meilleure volonté du monde. L'agent enquêteur a remonté la filière jusqu'à Revenu Canada (impôt).

Lorsqu'on lui a montré sa lettre, le fonctionnaire en cause a expliqué qu'il voulait simplement obtenir l'autographe de la journaliste. Il ne semblait pas poser le moindre danger pour elle. Soulagée, la journaliste a demandé que l'affaire soit abandonnée.

Toutefois, comme il avait appris que le fonctionnaire s'était servi de renseignements tirés des données de l'impôt, le Commissariat a dû en informer Revenu Canada, qui s'est donné un code d'éthique très strict à ce sujet et qui s'impose des mesures de sécurité radicales aux fins du traitement des dossiers des contribuables. Revenu Canada a fait enquête, conclu qu'il ne s'agissait pas d'un incident isolé et punit l'admirateur pour son inconduite.

Canada

Longs délais de traitement à Revenu

La Loi sur la protection des

renseignements personnels est maintenant en vigueur depuis huit ans, mais certains ministères continuent à faire fi des délais qu'elle impose. Revenu Canada (impôt), par exemple, témoigne parfois d'une souveraine indifférence quant au droit des demandeurs de recevoir les renseignements qu'ils réclament dans les délais prévus par la Loi. C'est vraiment paradoxal, puisqu'on sait avec quelle promptitude le fisc pénalise les contribuables qui produisent leur déclaration en retard...

Nous ne citerons qu'un exemple, celui d'une femme qui s'était rendue le 7 mai 1990 au bureau de l'impôt de Vancouver pour demander où en était la demande qu'elle avait présentée en janvier afin de voir son dossier d'impôt sur le revenu. Revenu Canada n'avait pas trace de sa première demande, de sorte que la femme en a déposé une seconde. Le 26 juin, elle a fini par téléphoner au Commissariat pour se plaindre de n'avoir pas eu la moindre nouvelle à ce sujet.

Même après que le Commissariat se soit enquis auprès de Revenu Canada (impôt) au sujet du délai, ce dernier n'a pourtant procédé à la communication que le 13 août 1990, soit 96 jours après le dépôt de la seconde demande. Les ministères peuvent demander une prolongation du délai de 30 jours dans certaines circonstances, mais ils doivent en informer le demandeur, qui peut alors porter plainte si la prolongation du délai lui semble déraisonnable.

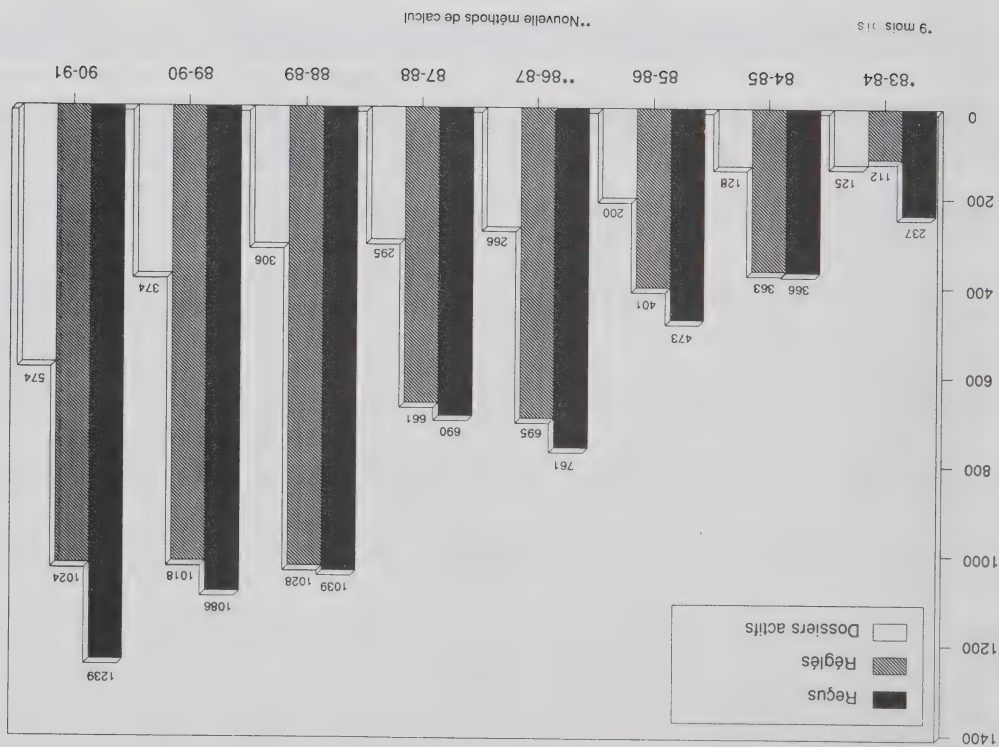
Résultats

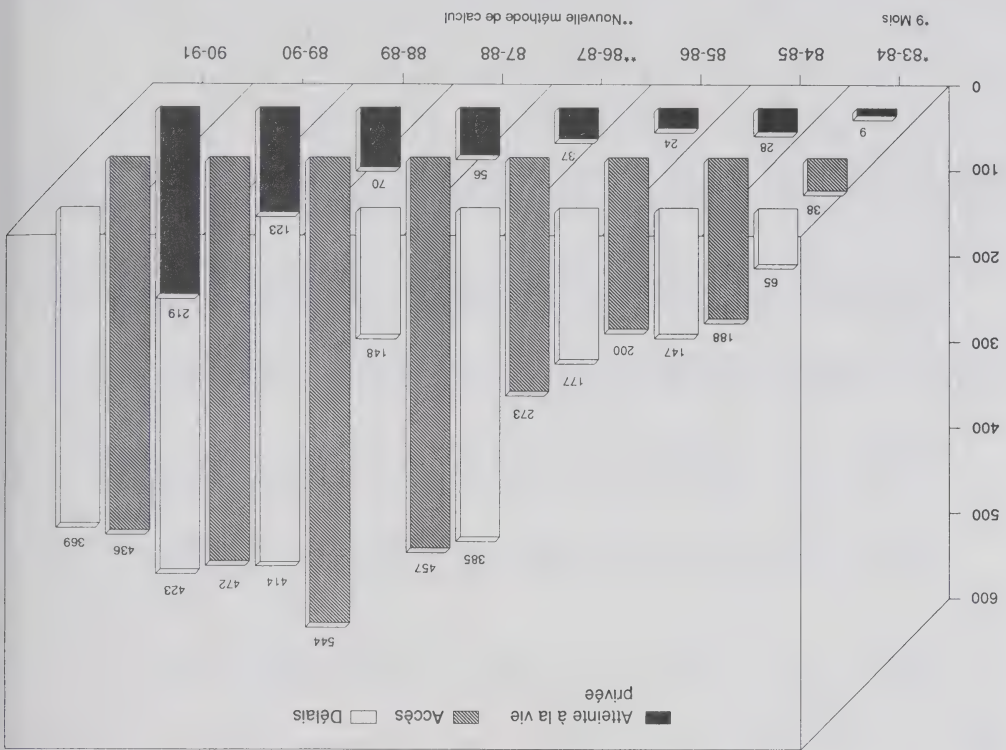
Ministère	NOMBRE	Bien fondée	Bien fondée; résolue	Non fondée	Abandonnée
ndarmerie royale du Canada	78	2	3	66	7
stice Canada	9	2	0	7	0
nnale royale canadienne	1	0	1	0	0
sées nationaux du Canada	1	0	0	1	0
ches et Océans	6	1	3	1	1
venu Canada, Douanes et Accise	14	11	1	2	0
venu Canada, Impôt	71	43	0	28	0
nté et Bien-être social Canada	34	16	3	15	0
crétariat d'Etat du Canada	3	2	0	1	0
vice canadien du renseignement de sécurité	83	6	9	67	1
vice correctionnel Canada	162	84	19	49	10
ciété canadienne des postes	233	13	39	171	10
ciété du crédit agricole Canada	1	0	0	1	0
ificiteur général Canada	14	1	0	12	1
istique Canada	1	0	0	1	0
nsports Canada	42	27	2	12	1
vail Canada	1	0	0	0	1
e maritime du Saint-Laurent	1	0	0	1	0
TAL	1,024	292	115	562	55

Plaintes Régées par Institutions et Résultats

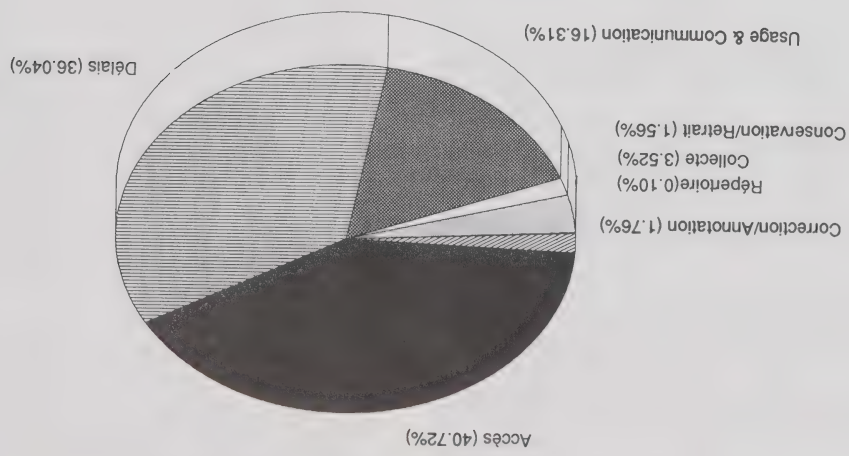
Ministère				Résultats	
NOMBRE	Bien fondée	Bien fondée; résolue	Non fondée	Abandonnée	
Anciens combattants Canada	5	3	0	2	
Affaires extérieures Canada	7	3	0	3	
Affaires indiennes et du Nord Canada	10	0	0	10	
Agriculture Canada	11	2	1	8	
Approvisionnement et Services Canada	3	0	2	1	
Archives nationales du Canada	24	1	3	19	
Bureau du Conseil privé	3	2	0	1	
Commissariat aux langues officielles	1	0	0	1	
Commission canadienne des droits de la personne	5	1	3	1	
Commission de la fonction publique du Canada	2	0	0	2	
Commission des plaintes du public contre la GRC	1	0	0	1	
Commission des relations de travail dans la fonction publique	7	0	3	4	
Commission nationale des libérations conditionnelles	20	2	5	13	
Conseil du Trésor du Canada	1	0	0	0	
Consommateurs et Sociétés	5	3	0	1	
Défense nationale	84	34	8	31	
Emploi et Immigration Canada	78	33	10	27	
Environnement Canada	1	0	0	1	
Finances Canada	1	0	0	1	

Nombre de dossiers 1983-1991





Plaintes réglées et motifs 1983-1991



Plaintes réglées par motifs 1990-91

Origine des plaintes réglées

Terre-Neuve	0
Ile-du-Prince-Édouard	8
Nouvelle-Écosse	41
Nouveau-Brunswick	36
Québec	148
Région de la Capitale nationale - Québec	6
Région de la Capitale nationale - Ontario	53
Ontario	407
Manitoba	66
Saskatchewan	33
Alberta	55
Colombie-Britannique	166
Territoires du Nord-Ouest	0
Yukon	5
Hors Canada	0
TOTAL	1,024

Si les ressources humaines et financières du Commissariat n'augmentent pas, le nombre de plaintes en souffrance grimpera à plus de 700 d'ici la fin de l'année en cours, soit à plus que le nombre total de plaintes ayant fait l'objet d'une enquête en 1987-1988.

Bien que sa productivité se soit améliorée, le Commissariat n'a pas fermé plus de dossiers cette année que l'an dernier. Son efficacité accrue a été plus que compensée par la baisse du nombre de plaintes concernant des retards, qui mobilisent moins de ressources que les autres, et par l'augmentation massive du nombre de plaintes concernant le code d'éthique sur les renseignements personnels, c'est-à-dire celles qui nécessitent les enquêtes les plus complexes et les plus longues.

Malheureusement, l'administration fédérale a rejeté les demandes du Commissariat, qui réclamait plus d'enquêteurs et plus de crédits de fonctionnement. Cette décision fera augmenter plus encore un arriéré déjà croissant, alourdira la charge des enquêteurs et prolongera la période d'attente des clients, qui veulent obtenir une décision sur leurs plaintes. Bref, le Commissariat lui-même risque désormais de devenir l'une des causes du problème.

RÉSULTATS									
MOTIFS		Bien fondée	Bien fondée; résolue	Non fondée	Abandonnée	TOTAL			
ACCÈS		30	70	320	16	436			
	Accès	27	69	305	16	417			
	Correction/Annotation	3	1	14	0	18			
	Répertoire	0	0	1	0	1			
	Langue	0	0	0	0	0			
ATTEINTE À LA VIE PRIVÉE		17	45	141	16	219			
	Collecte	0	11	22	3	36			
	Conservation/Retrait	3	4	7	2	16			
	Usage & Communication	14	30	112	11	167			
DÉLAIS		245	0	101	23	369			
TOTAL		292	115	562	55	1,024			

Les enquêteurs du Commissariat ont mené 1 008 enquêtes sur des plaintes (551 non fondées, 402 bien fondées et 55 abandonnées).

Cette année, les plaintes ont été groupées en trois grandes catégories, soit les plaintes concernant l'accès, c'est-à-dire les difficultés éprouvées par les citoyens désireux de consulter les dossiers qui les concernent; les plaintes portant sur la protection des renseignements personnels, c'est-à-dire le code d'équité en la matière (collecte, utilisation et divulgation conformes aux règles) et les plaintes concernant les retards, tant pour la première réponse à une demande que pour les prolongations de délai.

Même si les enquêteurs ont étudié plus de 1 000 plaintes au cours de l'exercice, ce qui correspond à la norme des trois dernières années, il en restait 589 en souffrance à la fin de l'année, soit une augmentation de 38 p. 100 par rapport à l'an dernier. Bref, le Commissariat se retrouve avec un arriéré après avoir trimé si dur, il y a deux ans, pour éliminer celui d'alors. Le problème s'aggravera encore si l'augmentation de 10 p. 100 du nombre de plaintes prévue pour 1991-1992 se concrétise, ce qui sera probablement le cas, s'il faut en croire l'augmentation de 14 p. 100 de cette année.

D'autres ressources, de grâce!

Selon ce critère, la Gendarmerie royale du Canada distance de loin les autres institutions fédérales par la qualité de son rendement, car 5 seulement des plaintes portées contre elle se sont révélées bien fondées ou bien fondées et résolues, tandis que 16 n'étaient pas fondées et que 7 autres ont été abandonnées. C'est une baisse importante par rapport aux 19 plaintes bien fondées d'il y a 2 ans et aux 10 de l'an dernier, qui reflète le respect sincère de la GRC pour l'esprit et la lettre de la Loi. Son coordonnateur de l'accès à l'information et de la protection des renseignements personnels mérite d'ailleurs des éloges pour son engagement personnel de réduire le nombre de plaintes bien fondées. Pour leur part, les Archives nationales continuent de maintenir leurs normes élevées, car 4 seulement des 23 plaintes portées contre elles se sont révélées bien fondées, et 3 des 4 ont été résolues. Au risque de friser l'inconséquence, nous devons aussi féliciter la Société canadienne des postes, qui s'est pourtant classée au premier rang pour le nombre de plaintes, puisque 50 seulement des 230 plaintes portées contre elle étaient bien fondées, et que 37 des 50 ont été résolues. Bien que le SCC semble avoir surmonté son problème de respect des délais, il conserve la pire proportion de plaintes bien fondées des grandes institutions fédérales, avec 64 p. 100 (103 sur 162). Sous cet aspect, Emploi et Immigration Canada et Revenu Canada (Impôt) se sont classés ex æquo au deuxième rang, avec 60 p. 100; le MDN les a suivis de près, avec 58 p. 100 de plaintes bien fondées.

Le nombre des plaintes portées contre la Société canadienne des postes est passé de 97 l'an dernier à 237 cette année, tandis que les 165 plaintes portées cette année contre le SCC représentent moins de la moitié du «record» de 392 établi l'an dernier. Une autre augmentation marquée s'est produite dans le cas d'Emploi et Immigration Canada, dont les 128 plaintes représentent le triple du total de l'an dernier pour cet organisme. Pour sa part, Transports Canada est revenu à un résultat plus près de la normale, avec 67 plaintes, alors qu'on n'en avait porté que 6 contre lui en 1989-1990. Il y a eu d'autres augmentations importantes du nombre de plaintes à l'endroit des Archives nationales, du MDN et du Service canadien du renseignement de sécurité (SCRS), sans qu'on sache très bien pourquoi. Par contre, le nombre de plaintes portées contre Santé et Bien-être social Canada et contre la GRC a baissé.

Prestation des institutions fédérales

Les plaintes peuvent être causées par plusieurs facteurs, comme une augmentation imprévue du nombre de demandes, tout simplement. En fait, une grande partie de ces facteurs sont totalement indépendants de la volonté des institutions responsables. La proportion des plaintes bien fondées est un indice plus significatif de la qualité de leur prestation.

Code d'éthique sur les
renseignements personnels

Bien que les plaintes portant sur des refus d'accès à l'information soient à la hausse, l'augmentation de 14 p. 100 constatée au cours de la dernière année est imputable à une importante poussée des plaintes concernant la collecte, l'utilisation et la divulgation des renseignements personnels, c'est-à-dire ce qu'on appelle un code d'éthique sur les renseignements personnels. Cette année, le nombre de plaintes de ce genre a grimpé en flèche, en établissant un record : 386, par rapport aux 173 de l'an dernier.

Une fois de plus, le problème semble être dû essentiellement aux conflits de travail à la Société canadienne des

Les dix grands

postes, qui donne l'impression d'appliquer sa nouvelle politique de gestion des congés avec beaucoup de fermeté. Les employés craignent qu'on ait recueilli indûment des renseignements médicaux qui les concernent et qu'on les ait utilisés pour gérer leur présence au travail.

Le rapport de cette année contient une liste des dix plus gros « clients » du Commissariat, qui totalisent 80 p. 100 de sa charge de travail. Le Service correctionnel du Canada, qui dominait depuis le début pour le nombre de nouvelles plaintes, n'a été que trop heureux de céder cet « honneur » en 1990-1991 à la Société canadienne des postes.

		MINISTÈRE		TOTAL	ACCÈS	RETARD	AUTRE	MOTIFS	
		Société canadienne des postes		239	40	54	145		
		Service correctionnel du Canada		165	77	50	38		
		Défense nationale		163	51	56	56		
		Emploi et Immigration Canada		128	61	44	23		
		Service canadien du renseignement de sécurité		77	67	9	1		
		Revenu Canada, Impôt		75	23	39	13		
		Transports Canada		67	43	17	7		
		Archives nationales du Canada		51	12	1	38		
		Gendarmerie royale du Canada		50	35	2	13		
		Santé et Bien-être social Canada		32	14	15	3		
		Autres		192	95	50	47		
		TOTAL		1,239	518	337	384		

Le nombre de plaintes a augmenté d'environ 10 p. 100 par année depuis que le Commissariat a fait ses débuts, il y a sept ans. La tendance s'est maintenue l'an dernier, car les 1239 plaintes reçues représentent une augmentation de 14 p. 100 par rapport aux 1086 de l'année précédente.

Plaintes portant sur la lenteur des réponses aux demandes

Dans ses rapports antérieurs, le Commissaire a parfois eu l'impression de faire un travail de Sisyphe, puisqu'il a dû constamment répéter ses critiques au sujet des longs délais de traitement des plaintes du Service correctionnel du Canada (SCC) et du ministère de la Défense nationale (MDN).

La façon du MDN de traiter les rapports d'évaluation du rendement était elle aussi la cause de nombreuses plaintes de retards. Le problème était dû au fait que les militaires devaient présenter une demande officielle pour avoir accès à leurs évaluations, ce qui créait une charge de travail énorme et entraînait fatalement un arriéré. L'an dernier, le Commissaire a applaudi à la décision du MDN de traiter ces demandes sans formalités. Comme il l'avait prévu, le nombre de demandes adressées au MDN en vertu de la Loi a baissé de 20 p. 100, et la plus grande partie de cette baisse est directement attribuable à ce changement de politique, qui a fait chuter de 36 p. 100 (de 78 à 50) le nombre de plaintes de retards portées contre le MDN.

Les institutions gouvernementales s'efforcent de toute évidence de respecter les délais imposés par la Loi, et la tendance le démontre sans équivoque. Néanmoins, la rarefaction des ressources risque de tuer ces progrès dans l'oeuf. Le droit du citoyen d'avoir accès rapidement aux renseignements personnels qui le concernent ne devrait pas être sacrifié sur l'autel des restrictions budgétaires.

Résultat? Une baisse étonnante de 200 p. 100 (de 214 à 50) du nombre de plaintes de ce genre portées contre le SCC. L'an dernier, ces plaintes à l'endroit du SCC représentaient 50 p. 100 de l'ensemble des plaintes portant sur les retards dont le Commissariat avait été saisi, et cette année, elles n'en représentent plus que 15 p. 100.

Chapeau pour un travail bien fait!

Être doctrinaire au point d'insister sur le caractère confidentiel de tous les cas risque de donner à la Loi une mauvaise réputation qu'elle ne mérite pas. Ces incidents mettant en cause le SCC en sont un bon exemple.

Bien que les raisons d'intérêt public invoquées par le SCC pour communiquer les deux rapports en question consistent à préserver la confiance que la population accorde au système correctionnel, il en a retiré des parties qui contiennent des critiques à l'endroit de certains membres de son personnel. Même si les mesures qu'il a prises pour protéger ces gens sont compréhensibles, le rapport «censure» qui en résulte ne donne pas au public un compte rendu complet de l'incident.

S'il ne communique pas ce qui le fait mal paraître aussi bien que ce qui l'avantage, le SCC agit-il vraiment pour des raisons d'intérêt public? C'est précisément cette question qui continue à faire l'objet de discussions entre ses dirigeants et le Commissaire à la protection de la vie privée. Il nous semble que le SCC devrait n'invoquer la clause «d'intérêt public» que dans des cas extraordinaires, et s'en servir alors pour communiquer une information complète.

N'oublions pas l'autre côté de la médaille: il est pour le moins inhabituel que le Commissaire à la protection de la vie privée rappelle publiquement aux institutions fédérales que le droit à la vie privée n'est pas absolu. Le fait est que la Loi reconnaît que la vie privée peut être violée si certains intérêts collectifs importants sont en jeu.

«La vérité, toute la vérité et rien que la vérité»

Cette histoire n'est pas finie, car le Comité des privilèges n'a pas terminé ses délibérations, et le Commissaire à la protection de la vie privée n'a pas non plus mené à bien son enquête sur une plainte connexe.

Le Commissaire par intérim à la protection de la vie privée a comparu devant le Comité des privilèges. Il a applaudi à la détermination du solliciteur général de protéger la vie privée des personnes mentionnées dans les rapports, mais il a conclu que le Ministre interprétait la Loi de façon trop restrictive. En effet, le sous-alinéa 8(2)m(i) lui donne de toute évidence le pouvoir de décider si la communication de la version intégrale des rapports au Comité de la Justice siègeant à huis clos sert l'intérêt public. Le Commissaire par intérim a ajouté qu'il n'était pas du tout contraire à l'esprit de cette disposition de la Loi que le Ministre juge d'intérêt la communication des renseignements au Comité, à condition qu'elle ait lieu dans des conditions garantissant la confidentialité des parties «sensurées».

Une fois que les renseignements ont été filtrés à la satisfaction du Commissaire du Service correctionnel et du Solliciteur général, ceux-ci avisent le Commissaire à la protection de la vie privée de leur intention de les communiquer (à l'avance, si c'est possible sans leur causer trop de difficultés). Quand le Commissaire reçoit le préavis, il décide s'il s'agit d'une communication pour des raisons d'intérêt public qui «justifieraient nettement une éventuelle violation de la vie privée». S'il n'est pas de cet avis, il en informe le SCC. Il convient toutefois de souligner que le Commissaire n'a pas le pouvoir d'empêcher la communication des renseignements, mais seulement de prévenir les personnes intéressées qu'ils seront divulgués.

Il est extrêmement difficile d'appliquer le critère des raisons d'intérêt public, comme on l'a vu dans deux cas de communications dont le Commissaire a fait état dans son rapport de l'an dernier («Communication des rapports portant sur l'évasion de deux détenus»). Le Comité permanent de la Justice et du Solliciteur général a tenu à se renseigner sur les événements ayant entouré ces deux incidents qui avaient fait la manchette, à savoir l'évasion du pénitencier de Dorchester, au Nouveau-Brunswick, d'un dénommé Allan Légère (qui aurait assassiné une personne après son évasion) et celle de Daniel Gingras, qui avait profité d'une permission de sortie d'une journée pour s'enfuir. Par la suite, il avait assassiné deux personnes.

Le SCC avait déjà communiqué aux médias des versions épurées des rapports d'enquête, et c'est cette version des rapports qu'il a remise au Comité. Toutefois, celui-ci a réclamé les versions intégrales, et il a ordonné au Solliciteur général de les lui faire remettre.

Le Solliciteur général a refusé d'obéir, en alléguant que la *Loi sur la protection des renseignements personnels* lui interdisait de communiquer les renseignements demandés. Son refus a fait l'objet d'une question de privilège à la Chambre des communes, et la question a fini par être renvoyée au Comité permanent des privilèges et des élections. Dans son témoignage devant le premier Comité, le Solliciteur général a déclaré qu'il était tenu de respecter le sous-alinéa 8(2)(i) de la *Loi sur la protection des renseignements personnels*, de sorte que, avant de communiquer les renseignements demandés, il devait être convaincu qu'il était essentiel de le faire pour des raisons d'intérêt public qui justifieraient clairement une éventuelle violation de la vie privée. Il a ajouté qu'il n'était pas sûr que la *Loi sur la protection des renseignements personnels* l'autorisait à accéder à la demande du Comité, qui voulait étudier à huis clos la version intégrale des rapports.

La protection de la vie privée et l'intérêt public: un équilibre difficile à protéger

Globalement, la *Loi sur la protection des renseignements personnels* interdit aux institutions fédérales de communiquer les renseignements personnels qui sont sous leur contrôle à défaut du consentement de la personne concernée. Toutefois, la Loi admet aussi treize exceptions à la règle.

L'une des treize est de portée très générale, ce qui la rend difficile à appliquer et ouvre la porte à de nombreux abus. C'est le sous-aligné 8(2)(1), qui autorise la divulgation des renseignements personnels à toutes les fins autres que celles auxquelles ils ont été recueillis, dans les cas où, de l'avis du responsable de l'institution:

des raisons d'intérêt public justifieraient nettement une éventuelle violation de la vie privée...

Au cours de la dernière année, l'institution qui a le plus fréquemment invoqué cette disposition a été le Service correctionnel du Canada (SCC). Le problème se pose quand des incidents survenus dans le contexte carcéral, comme des évasions, des morts violentes ou des prises d'otages, mènent à des enquêtes internes qui aboutissent à des rapports contenant des renseignements personnels à la fois sur les détenus et sur les fonctionnaires impliqués du SCC.

Par conséquent, le SCC doit tenir compte des interdictions imposées par la *Loi sur la protection des renseignements personnels* avant de communiquer ces rapports. Il se peut fort bien qu'il veuille les distribuer afin de conserver la confiance que le public accorde au système correctionnel, et il peut aussi avoir besoin d'en fournir des exemplaires aux journalistes qui les ont réclamés en vertu de la *Loi sur l'accès à l'information*, ainsi qu'à des députés et sénateurs ou à des comités parlementaires désireux de les étudier afin d'évaluer la qualité globale de l'administration correctionnelle. Dans ces cas-là, le SCC retire des rapports tous les renseignements considérés comme inconsultables en vertu de la *Loi sur l'accès à l'information*, de même que les détails personnels délicats ou non pertinents.

Bref, le SCC s'efforce de divulguer seulement les renseignements personnels nécessaires pour satisfaire au critère d'intérêt public établi par la *Loi sur la protection des renseignements personnels* et pour donner au public une image claire de ce qui s'est passé.

Enfin, la Loi sur la protection des renseignements personnels interdit l'accès aux autres bases de données fédérales en vue de la création d'une liste de ce genre, dont l'établissement nécessiterait la promulgation d'une loi fédérale qui la soustrairait à l'application de la Loi sur la protection des renseignements personnels. Le Commissaire n'appuierait jamais une démarche pareille.

Les citoyens du monde entier en ont assez d'être comptés, enregistrés et contrôlés par l'Etat. La création d'une liste permanente des électeurs risque de susciter un profond malaise. Il serait ironique que le processus électoral, qui est le fondement même de la démocratie, devienne un mécanisme qui fera pencher la balance plus encore du côté de l'Etat, aux dépens du citoyen.

Le Commissaire ne veut pas s'opposer au progrès, mais il tient à poser des questions pertinentes avant que ce projet n'aille trop loin. Ses observations ont été bien accueillies par la Commission d'enquête, qui se propose de rendre son rapport public à l'automne de 1991.

La réforme électorale: une liste électorale permanente

Il peut être question de vie privée quand on s'y attend le moins, comme lorsque le gouvernement a chargé une Commission royale d'enquête d'étudier l'opportunité d'une refonte de la législation électorale canadienne.

La Commission d'enquête devait étudier la procédure électorale et les modalités de financement des partis et des campagnes, ainsi que la possibilité d'une liste électorale permanente grâce à laquelle nous n'aurions plus besoin chaque fois d'une énumération de porte à porte.

L'élimination de l'énumération de porte à porte aurait des avantages. Toutefois, la solution envisagée touchant cette pratique qui prend du temps et qui gonfle le coût déjà élevé des élections fédérales au Canada ne doit pas être adoptée à la légère.

La Commission a entendu des propositions axées sur des combinaisons de renseignements provenant de divers fichiers d'information fédéraux, comme les dossiers de l'impôt sur le revenu, les registres de la citoyenneté, les avis de changement d'adresse de la Société canadienne des postes, les formulaires de recensement et les registres des pensions. On devait aussi présenter d'autres propositions fondées sur l'intégration des registres provinciaux de la santé et des dossiers des conducteurs. Enfin, l'idée d'obliger les électeurs à avoir une carte d'identité spéciale ou à produire leur numéro d'assurance sociale (NAS) a séduit beaucoup de monde.

chaque citoyen.

Tout cela a incité le Commissaire à la protection de la vie privée à écrire à la Commission d'enquête pour lui demander de réfléchir aux répercussions éventuelles de ses recommandations sur la vie privée. Le Commissaire s'inquiète des applications des nouvelles collections (ou couplages) de renseignements personnels sur une grande échelle. Une liste électorale permanente comme celle qu'on envisage deviendrait une sorte de registre de la population qui serait vraiment dangereux pour les droits et libertés de la personne. L'expérience acquise en temps de guerre prouve que, même au Canada, on fera mauvais usage de ces listes, pour traiter injustement des groupes importants de citoyens et pour les arrêter, les emprisonner et confisquer leurs biens.

En outre, s'il fallait que cette liste existe, il y aurait des pressions croissantes pour qu'elle soit mise à la disposition de tous les organismes gouvernementaux imaginables, à des fins qui n'auraient rien à voir avec les élections. Il faudrait absolument que son utilisation soit limitée à cette seule fin, et que les données qu'elle contiendrait soient strictement confidentielles.

Le mécontentement croissant que suscitent les utilisations injustifiées du NAS reflète la résistance des citoyens aux projets d'identification et d'enregistrement à l'échelle nationale, et cette résistance se renforcerait si l'on devait se servir du NAS pour faire le pont entre différentes bases de données et pour confirmer le droit de vote de

Le dépistage génétique est sur le point de devenir une question centrale dans les domaines de la reproduction humaine (dépistage avant la conception et dépistage prénatal et néo-natal), de l'emploi (filtrage et contrôle), de l'accès aux services gouvernementaux et privés (éducation, assurances, crédit), des enquêtes criminelles, des soins médicaux de routine et de la recherche.

Les énormes possibilités actuelles et potentielles d'utilisation de l'information obtenue grâce au dépistage génétique ont amené le Commissaire à étudier ses implications pour la protection de la vie privée. Il devrait avoir terminé son étude à la fin du printemps de 1991. Toutefois, il semble qu'une conclusion s'impose déjà. Le dépistage génétique a de telles implications pour la protection de la vie privée que le gouvernement doit se demander s'il devrait directement réglementer son utilisation dans le secteur privé.

2) Contrôle génétique: Recherche de changements génétiques ou chromosomiques pouvant résulter de l'exposition dans le milieu du travail ou dans le milieu ambiant à des substances chimiques ou à divers phénomènes (radiation ou émanations de matières plastiques, par exemple).

3) Analyse pathologique de l'ADN: Appelée communément, identification par l'ADN. Cette technique consiste en une comparaison génétique d'échantillons. C'est ainsi qu'on peut prouver que la composition génétique du sang trouvé sur le lieu d'un crime correspond à celle du sang d'un suspect. Ce genre d'analyse peut aussi prouver l'affiliation génétique dans les affaires d'immigration ou de paternité.

Les autres formes d'analyse biotechnologique, comme le dépistage des anticorps du VIH et du SIDA ou des drogues ne révèlent qu'un seul fait, l'infection au VIH ou la consommation de drogues dans le passé. Le dépistage génétique, par contre, peut révéler des centaines de données sur un individu ou sur ses parents, de la certitude d'être atteint d'une maladie ou d'une affection invalidante ou mortelle, comme la chorée de Huntington ou la fibrose kystique, jusqu'au risque de développer des troubles psychiatriques, comme d'être maniaque-dépressif, ou d'être prédisposé à avoir des taux élevés de cholestérol, à faire de l'hypertension ou à être atteint de certains types de cancer.

En fait, la plupart des programmes de dépistage antidrogue continuent de préoccuper le Commissaire, qui estime que les programmes gouvernementaux sont un mauvais exemple pour le secteur privé, et que, dans la plupart des cas, ils ne semblent pas conformes à la Loi sur la protection des renseignements personnels. Il reste que le Commissariat n'a pas de meilleurs recours que de critiquer publiquement ces programmes, car il ne peut contraindre l'administration fédérale à respecter la Loi.

Le dépistage du VIH

Le personnel du Commissariat continue à répondre aux demandes d'information et à faire enquête sur les plaintes concernant le respect de la vie privée dans le contexte du VIH et du SIDA. Étant donné que les demandes portent souvent sur des questions ou sur des organismes qui ne relèvent pas de la Loi sur la protection des renseignements personnels, le personnel tente d'aligner les appels vers les autorités responsables.

La pierre angulaire du travail du Commissariat en matière de VIH et de SIDA est un rapport publié en 1989 et intitulé *Le SIDA et la Loi sur la protection des renseignements personnels*. Le personnel a en outre contribué à l'élaboration des «Guidelines on Ethical and Legal Considerations in Anonymous Unlinked HIV Seroprevalence Research», en 1988. Ces lignes directrices ont été publiées dans le *Canadian Medical Journal*, en 1990. En février 1991, le Commissariat a participé à la révision des lignes directrices originales.

Le dépistage génétique

La génétique moderne nous offre de grandes possibilités d'identification des troubles génétiques, dont quelques-uns susceptibles d'être traitables. Toutefois, le dépistage génétique soulève de graves questions de protection de la vie privée, en ce qu'il risque de révéler des renseignements très délicats sur la personne qui subit les tests et sur ceux et celles qui partagent son bagage génétique. Les tests de dépistage de ce genre font appel à trois techniques.

1) Filtrage génétique: Examen d'un échantillon de tissu ou de sang d'un individu pour y dépister les gènes ou «marqueurs» génétiques indiquant la présence ou le risque d'un trouble génétique ou d'une autre caractéristique physique.

Et ce n'est pas tout. Condition physique et Sport amateur a réagi au rapport Dublin sur la consommation de drogues chez les athlètes amateurs en mettant sur pied une nouvelle organisation antidopage financée essentiellement par l'administration fédérale, quoique n'en faisant pas partie. Cette organisation doit coordonner tous les plans antidopage dans le domaine du sport et administrer un programme d'envergure accrue pour soumettre les athlètes à des tests de dépistage des substances prosrites.

L'un des éléments fondamentaux du plan envisagé consiste à soumettre les athlètes à des tests de dépistage «à l'improviste», indépendamment des compétitions. En fait, on prévoit jusqu'à 3000 tests (par année, sans doute), dont la majorité seraient faits «à l'improviste.».

Comme l'organisation antidopage ne sera pas un organisme fédéral, la Loi sur la protection des renseignements personnels ne s'y appliquera pas. Il se peut qu'on ait délibérément opté pour cette solution afin de contourner la Loi, mais l'approche de l'organisation, telle que le Ministre responsable l'a annoncée, soulève fatalement des objections fondées sur le respect de la vie privée. Les athlètes risquent de se retrouver à peu près complètement privés de droits à cet égard, à telle enseigne que le Commissaire a l'intention d'en discuter avec les responsables de Condition physique et Sport amateur.

L'obligation de subir des tests de dépistage des drogues dans ces conditions est contraire à la Loi sur la protection des renseignements personnels et elle risque d'être interdite pour peu qu'elle soit contestée en vertu de la Charte canadienne des droits et libertés. Bref, ces tests ne devraient être administrés que si l'on a des motifs raisonnables de croire que quelqu'un consomme de la drogue - ou encore après un accident.

Il est regrettable de constater que le ministère de la Défense nationale (MDN) soit toujours bien déterminé à appliquer son projet d'astreindre les militaires à des tests de dépistage des drogues et ce, en dépit des recommandations du Commissaire et des conclusions du comité des transports sur le dépistage obligatoire effectué au hasard. Cela dit, le MDN compte faire subir des tests lorsqu'il aura des motifs valables de le faire, dans le cadre d'enquêtes menées à l'occasion d'un accident ou d'un incident, pendant une période de surveillance à la suite d'un test de dépistage des drogues s'étant révélé positif, et enfin pour recueillir des données. Il prévoit de plus administrer des tests obligatoires au hasard dans le cas des militaires affectés à des unités opérationnelles ou occupant des postes reliés à la sécurité.

Le dépistage antidrogue

Les lecteurs assidus du rapport annuel se rappelleront que, l'an dernier, le Commissaire avait fortement déconseillé à l'administration fédérale de généraliser le dépistage antidrogue pour contre le fléau des substances interdites.

Dans son étude en profondeur, intitulée *Le dépistage antidrogue et la vie privée*, le Commissaire a examiné différents milieux, notamment ceux des transports, des établissements correctionnels, des forces armées et des sports. Il a constaté qu'un grand nombre de projets de dépistage envisagés par l'administration fédérale risquaient de violer la *Loi sur la protection des renseignements personnels* et la *Charte canadienne des droits et libertés*, voire des principes plus fondamentaux encore de protection de l'intégrité individuelle.

Il est clair que la situation a évolué depuis, et qu'on envisage des mesures de protection de la vie privée, qui était menacée par le dépistage antidrogue. Le Commissariat a été consulté par Santé et Bien-être social Canada au sujet d'éventuels protocoles de dépistage. Il a répondu au rapport de l'administration fédérale sur le dépistage antidrogue dans le secteur des transports, et il a discuté avec le Service correctionnel du Canada (SCC) le règlement que celui-ci a proposé en vue du dépistage antidrogue dans les pénitenciers fédéraux.

Transports Canada n'envisage plus de soumettre au hasard tous les titulaires de postes reliés à la sécurité des transports à un test de dépistage des drogues obligatoire. Le dernier projet de règlement du SCC est de loin préférable aux versions antérieures, qui avaient été rejetées en 1989 par la division de première instance de la Cour fédérale, dans *Jackson*. Enfin, les protocoles de dépistage de Santé et Bien-être social Canada prévoient désormais des méthodes de prélèvement d'échantillons d'urine qui portent moins atteinte à la vie privée qu'auparavant.

Malheureusement, certains aspects de la politique de dépistage antidrogue dans le secteur des transports restent inquiétants. Transports Canada tient toujours à imposer des tests d'analyse d'urine préalablement à l'emploi pour les employés nouvellement recrutés ou mutés, ainsi qu'à l'occasion des examens médicaux périodiques, et cela même si ses propres recherches n'ont révélé aucune consommation sérieuse de substances pouvant représenter une menace pour la sécurité dans ce secteur. Il faut ajouter que l'analyse d'urine ne fournit que des renseignements très limités, à savoir qu'une personne a consommé telle ou telle substance dans un passé récent, sans préciser avec quelle fréquence et sans non plus confirmer que les facultés du sujet étaient altérées au moment du test, ou, chose plus importante encore, si elles le sont encore maintenant.

L'ACMD a communiqué ses activités
dans ce domaine au Commissaire, qui
se fera un plaisir de poursuivre le
dialogue avec elle.

Le code de l'ABC garantit aux clients le droit d'accès aux renseignements personnels qui les concernent et le droit aussi de les faire corriger. En outre, il contrôle les modalités de collecte, de conservation, d'utilisation, de divulgation, d'élimination et de sécurité applicables aux dossiers des clients. Les banques ont toujours su admirablement protéger la confidentialité de l'information relative à leurs clients, mais il reste que le code assurera désormais aux clients un meilleur contrôle des renseignements financiers qui les concernent. Cela dit, les promoteurs de la protection de la vie privée, dont le Commissaire, ont constaté quelques lacunes; par exemple, le code de l'ABC ne donne pas aux clients l'accès aux opinions ou aux jugements à leur endroit qui figurent dans leur dossier, mais seulement aux renseignements factuels sur eux-mêmes. Le Commissaire espère que le code sera modifié afin de combler les carences. Malgré ces réserves, le Commissaire perçoit d'une manière positive les efforts fournis par l'ABC. Bell Canada mérite des éloges, elle aussi, car elle s'est donné un code de protection des renseignements personnels qui reconnaît des droits et assure une protection à ses employés tout autant qu'à ses clients, et qu'elle ne limite pas leur accès aux seules données factuelles.

Dans un monde où les télécommunications font l'objet d'une concurrence de plus en plus féroce, ce souci manifeste de protéger la vie privée des clients et des employés aura sûrement un effet d'entraînement. Le Commissaire presse les autres entreprises du secteur des télécommunications d'emboîter le pas à Bell. Il suivra la situation et signalera les progrès réalisés. Enfin, l'Association canadienne du marketing direct (ACMD) a récemment annoncé l'adoption de nouvelles mesures de protection de la vie privée, en lançant son «Opération intégrité», le 13 février 1991. L'ACMD a renforcé les dispositions de protection de la vie privée de son code d'éthique, en s'engageant à donner aux consommateurs de meilleurs moyens d'échapper aux intrusions dans leur vie privée des entreprises d'envois postaux directs et de télémarketing. L'Opération intégrité donne aux consommateurs la possibilité de demander que leur nom soit rayé des listes d'envois postaux et des répertoires téléphoniques des membres de l'ACMD. En outre, elle interdit à ceux-ci d'inclure dans les listes qu'ils louent des renseignements de nature délicate (médicaux, financiers ou judiciaires, ou encore sur des questions d'assurances). L'ACMD a aussi mis sur pied un groupe de travail formé de représentants en vue de son secteur d'activité, qui étudieront les implications du marketing direct en matière de protection de la vie privée, afin d'élaborer d'autres politiques sur le transfert de données.

Toutes les instances européennes intensifient leur coopération et de développement économiques (OCDE), le Conseil de l'Europe, la CEE et les organismes européens de protection des données - sont parfaitement conscients des implications du projet de directive pour les pays qui ne sont pas membres de la CEE. Elles savent que le Canada - et les Etats-Unis, à ce compte-là - reconnaissent les principes applicables à la protection des données (le Canada a signé les lignes directrices de l'OCDE sur la protection des renseignements personnels). Elles savent aussi que les autorités gouvernementales nord-américaines préfèrent laisser le secteur privé s'autoréglementer.

Toutefois, les Européens n'ignorent pas que l'autoréglementation n'a pas connu de succès retentissants, et que seule une poignée d'entreprises canadiennes et américaines ont adopté des codes valables de protection des données.

Bref, même si les Européens reconnaissent qu'il peut y avoir plus d'une façon d'assurer la protection des données, par exemple grâce à des codes d'autoréglementation entre eux, ils ne sont pas disposés à accepter de compromis sur le plan des principes. Par conséquent, les organismes européens de protection des données n'autoriseront plus le transfert des renseignements personnels à des pays qui n'adhèrent que du bout des lèvres au principe de la protection de ces renseignements.

C'est un avertissement en bonne et due forme que le Commissaire à la protection de la vie privée du Canada s'est fait servir par les responsables européens de la protection des renseignements personnels.

L'an dernier, le Commissaire a recommandé dans son rapport annuel *protection des renseignements personnels* pour obliger les entreprises privées de compétence fédérale à élaborer, à enregistrer et à mettre en vigueur des codes de protection de la vie privée fondés sur les principes internationaux reconnus qui ont été établis par les lignes directrices de l'OCDE.

Ses discussions avec les autorités européennes chargées de la protection des données ont convaincu le Commissaire que des codes d'autoréglementation seraient acceptables, à condition de reposer sur une base juridique comme celle-là.

Il s'ensuit que, pour le Commissaire, la mise en oeuvre de cette recommandation est urgente, car non seulement les Canadiens méritent-ils de bénéficier de toute cette protection de leur vie privée, mais encore les entreprises canadiennes risquent-elles d'être sérieusement désavantagées lorsqu'elles voudront continuer après 1992 à traiter avec des firmes de l'Europe.

Des débuts encourageants

Il ne faut pas passer les réussites du secteur privé sous silence du seul fait qu'elles sont rares. Ainsi, en décembre 1990, l'Association des banquiers canadiens (ABC) a approuvé un code de protection des renseignements personnels digne d'être cité en exemple, dans lequel elle a précisé les normes minimales de protection des renseignements personnels des clients, que ses membres sont tenus d'appliquer.

La protection de la vie privée dans le secteur privé

Dans notre société où règne l'ordinateur, la distribution de l'information est illimitée. Et pourtant, le Canada se contente d'une législation qui assure une certaine protection contre les utilisations abusives de l'information dans l'administration fédérale et dans une partie des administrations provinciales, sans aucun mécanisme équivalent dans le secteur privé.

En Europe, la situation est très différente. La plupart des pays membres de la Communauté économique européenne (CEE) se sont donné des mécanismes de protection des renseignements personnels tant dans le secteur privé que dans le secteur public. En outre, les autorités s'efforcent actuellement pour renforcer et harmoniser ces mécanismes en vue de l'unification de l'Europe, en 1992. Pourquoi comparer le Canada à l'Europe? Eh bien, parce que ces différences ont d'importantes conséquences pour les entreprises canadiennes qui font des affaires en Europe... ou qui espèrent en faire. En effet, si le Canada n'adopte pas de législation comparable à la leur pour assurer la protection des données dans le secteur privé, les pays européens risquent de ne plus autoriser le transfert au Canada d'information concernant leurs ressortissants. La législation européenne sur la protection des données pourrait devenir une barrière non tarifaire qui réduirait nettement les possibilités des entreprises canadiennes de traiter avec ce qui promet de devenir l'un des plus grands blocs commerciaux du monde.

- éliminer tous les obstacles au libre échange de données personnelles entre les pays membres.

Le hic, c'est que la directive a des implications alarmantes pour les pays qui ne sont pas membres de la CEE et qui n'assurent pas une protection de la vie privée satisfaisant aux normes européennes. En effet, l'article 24 du projet de directive interdit aux membres de transférer des données personnelles à toute compétence qui n'en assure pas une protection satisfaisante. Compte tenu de la loi en ce moment, il est fort peu probable que le secteur privé au Canada puisse démontrer un niveau acceptable de protection de renseignements.

- établir un mécanisme assurant une protection uniforme et de qualité de la vie privée tant dans les secteurs public que privé;
- objectifs globaux:
- Le danger est très réel: il suffit pour en être convaincu d'étudier le projet de directive de la CEE sur la protection des données personnelles des individus, présenté en juillet 1990. Si ce projet est adopté, tous les pays membres de la CEE devront l'appliquer à partir du 1^{er} janvier 1993. La directive a deux

Dans certaines instances, notamment en Californie, les législateurs ont adopté des lois interdisant à la fois l'interception des communications cellulaires et la vente ou l'achat d'un dispositif d'écoute capable de les capter. Le Congrès des Etats-Unis est même saisi d'un projet de loi d'une portée plus vaste encore sur les communications informatiques et radio (H.R. 3378 et S. 1667). En vertu de ce projet de loi, il serait illégal d'intercepter une conversation transmise par un téléphone d'auto, à l'instar de toute autre communication radio privée.

Bien sûr, la loi ne peut pas nous assurer que nos conversations par téléphone cellulaire demeureront privées. En fait, certains prétendent que l'adoption d'une loi qui nous offrirait cette protection pourrait inspirer aux utilisateurs de ces téléphones un faux sentiment de sécurité, ce qui serait tout à fait contraire à l'intention du législateur. Le Commissaire n'est pas d'accord; selon lui, il est absolument vital que le Parlement agisse rapidement pour protéger la vie privée des utilisateurs de téléphones cellulaires. L'élimination des fils téléphoniques ne doit pas entraîner celle de la protection de notre vie privée.

Cette disposition peut recevoir différentes interprétations dans des cas précis, mais elle ne peut absolument pas être interprétée de façon à justifier la collecte de renseignements personnels d'une façon qui, autrement, serait illégale. En outre, toute collecte de renseignements personnels contraire à la *Charte* entreint aussi la *Loi sur la protection des renseignements personnels*.

La *Loi sur la protection des renseignements personnels* entre en jeu lorsque des organismes d'enquête fédéraux interceptent des conversations faites par téléphone cellulaire. C'est pour cette raison que le Commissaire tient à s'assurer que toutes les interceptions effectuées par des organismes fédéraux le sont conformément à la Loi.

Le Commissaire fait enquête sur cette question, et il compte publier les résultats de ses travaux dans son prochain rapport annuel.

Ce qu'il y a de plus inquiétant encore, selon le Commissaire, c'est l'absence de contrôle légal portant sur les interceptions par les citoyens des conversations transmises par téléphone cellulaire. Un commentateur a décrit la situation en ces termes:

L'utilisateur moyen d'un téléphone cellulaire est peut-être prêt à accepter d'entendre une autre conversation sur sa ligne, mais il serait probablement secoué d'apprendre que l'on peut délibérément écouter des conversations avec un équipement aussi simple qu'un vieux téléviseur capable de capter la fréquence UHF des téléphones cellulaires. (*Network Newsletter*, Vol. 10, n° 24, 30 juillet 1990, p. 1)

La Cour suprême a réuni un ensemble de dispositions juridiques protégeant les citoyens contre l'écoute de leurs conversations téléphoniques cellulaires par des agents de l'État, mais la *Charte* ne contient rien qui puisse contrôler le comportement d'un particulier. En outre, il est loin d'être sûr que les dispositions du *Code criminel* qui interdisent l'interception secrète des communications privées s'appliquent aux communications téléphoniques cellulaires. Après tout, ces communications sont transmises par radio et, par conséquent, il se peut qu'elles ne puissent être considérées comme « privées ».

Les Canadiens ont appris - parfois douloureusement - que les conversations faites par téléphone cellulaire peuvent être interceptées.

En Colombie-Britannique, un ministre provincial a démissionné après (qu'un journal?) eut imprimé des extraits de conversations téléphoniques qu'il avait eues dans sa voiture. Certaines des délégations provinciales à la conférence constitutionnelle du lac Meech soupçonnaient que leurs communications par téléphone cellulaire avaient été interceptées. Une Société provinciale d'énergie s'est retrouvée dans l'embarras quand quelqu'un a intercepté et publié les propos qu'un de ses employés avait tenus sur des leaders de la communauté à son téléphone cellulaire.

Face à cette nouvelle menace pour la vie privée, le Commissaire s'est posé deux questions:

- La Loi sur la protection des renseignements personnels protège-t-elle les conversations téléphoniques cellulaires?

- Les institutions fédérales, et notamment les organismes fédéraux d'application de la loi, restent-ils toujours dans la légalité lorsqu'ils interceptent des conversations de ce genre?

La Cour suprême a clairement déclaré que, lorsqu'ils n'ont pas obtenu l'autorisation judiciaire voulue, les agents de l'État ne peuvent pas soumettre les citoyens à une forme quelconque d'écoute électronique. S'ils le faisaient, ils se rendraient coupables de «perquisitions ou de saisies abusives». En effet, ils nous priveraient de notre droit à une protection raisonnable de notre vie privée, ce qui constituerait une violation de l'article 8 de la Charte canadienne des droits et libertés.

L'État ne peut plus présumer qu'un citoyen a renoncé à son droit à la protection de sa vie privée simplement parce qu'il «court le risque» d'être mis sous surveillance, par exemple en utilisant un mode de communication qu'il sait susceptible d'être intercepté. La Cour suprême a jugé que cette présomption fait courir un plus grand risque à notre société, en ce sens que si les agents de l'État pouvaient faire de la surveillance électronique sans mandat approprié, ils porteraient un si dur coup à la protection de notre vie privée que notre société ne pourrait plus être libre et ouverte.

Cette conclusion du plus haut tribunal du pays a des implications directes pour la Loi sur la protection des renseignements personnels, qui impose de nombreuses restrictions à la collecte des renseignements personnels par une institution fédérale, la principale (article 4) étant que seuls les renseignements «...qui ont un lien direct avec ses programmes ou ses activités» peuvent être recueillis par l'institution.

À l'heure actuelle, contrairement à la surveillance électronique, il n'existe aucune procédure par laquelle la police doit obtenir une autorisation pour faire de la surveillance magnétoscopique. La Cour suprême était très consciente de l'entrave que sa décision allait imposer aux policiers, mais elle n'en a pas moins jugé que seul le Parlement devrait décider dans quelles circonstances ils peuvent porter atteinte à la vie privée en ayant recours à la surveillance magnétoscopique.

Le juge La Forest l'a bien dit:

Selon moi, les tribunaux négligeraient leur rôle de protecteurs de nos libertés fondamentales s'ils devaient usurper le rôle du législateur et prétendre sanctionner la surveillance magnétoscopique en adoptant à cette fin un code de procédure conçu pour une technologie de surveillance complètement différente. C'est au législateur et à lui seul qu'il revient d'établir les conditions dans lesquelles les organismes d'application de la loi peuvent avoir recours à la technologie de surveillance magnétoscopique pour combattre la criminalité. Il en est de même pour toute nouvelle technologie que le progrès de la science mettra à la disposition de l'Etat dans les années à venir.

(p. 23)

Il est certain que le gouvernement légitimera pour que la police puisse obtenir l'autorisation judiciaire d'avoir recours à la surveillance magnétoscopique. Ce serait la façon logique de procéder, étant donné que personne ne conteste que, pour appliquer la loi, il faut pouvoir avoir recours à ce moyen de surveillance. Toutefois, comme il le fait pour la surveillance électronique, le Commissaire à la protection de la vie privée invite instamment le Parlement à faire en sorte que toute procédure qu'il adoptera face à l'obtention d'une autorisation judiciaire pour fins de surveillance magnétoscopique, protège la vie privée des innocents.

Par suite de l'arrêt *Wong*, les tribunaux ne peuvent plus se fonder sur le critère de l'analyse fondée sur le «risque couru» par la personne qui fait l'objet de la surveillance non autorisée. Comme le juge La Forest l'a déclaré :

... la vie privée serait mal protégée si le caractère raisonnable de notre attente en matière de respect de la vie privée dépendait de la question de savoir si nous sommes exposés à la surveillance électronique. Compte tenu de l'état avancé de la technologie en matière de surveillance, ce serait adopter une norme dépourvue de signification juridique, en dernière analyse, les ressources technologiques dont disposent les agents de l'État sont telles que nous courons maintenant le risque de voir nos propos enregistrés pratiquement chaque fois que nous parlons à une autre personne. (p. 7-8)

Par conséquent, même si l'accusé avait distribué de nombreuses invitations à se rendre à sa chambre d'hôtel et qu'il y avait donné accès à des inconnus, il n'avait pas perdu son droit au respect raisonnable de sa vie privée. La Cour suprême a clairement précisé que, même si l'on pourrait avoir recours sans mandat à la surveillance magnétoscopique des personnes qui se livrent à des activités illégales dans leurs chambres d'hôtel, la société s'opposerait à ce qu'on impose ce risque à tous ceux qui louent une chambre. Pour éviter ce risque, la Cour a jugé qu'elle devait interdire cette forme de surveillance.

En appel, la Cour suprême a tranché la question à six contre un en adoptant une autre position. La Cour concluait qu'en l'absence d'une autorisation judiciaire, la surveillance magnétoscopique constituait une violation de l'article 8 de la *Charte*, qui garantissait le droit à la protection contre les fouilles, les perquisitions ou les saisies abusives. L'arrêt est particulièrement remarquable en ce qu'il élargit la définition du droit à la vie privée en y englobant celui de ne pas faire l'objet d'une surveillance magnétoscopique systématique par des agents de l'État. La Cour suprême a conclu que le droit à la vie privée doit être protégé par des instances judiciaires indépendantes, et qu'on ne peut laisser la police décider quand avoir recours à la surveillance magnétoscopique.

Dans les motifs de jugement de la majorité, le juge La Forest a précisé clairement que toutes les formes de surveillance électronique auxquelles des agents de l'État ont recours sans autorisation judiciaire constituent des violations de l'article 8 de la *Charte* :
... le droit général à la protection contre les fouilles, les perquisitions ou les saisies abusives garanti par l'art. 8 doit évoluer au rythme du progrès technologique et, par conséquent, nous assurer une protection constante contre les atteintes non autorisées à la vie privée par les agents de l'État, peu importe la forme technique que peuvent revêtir les divers moyens employés. (p. 6)

des innocents court lorsque la police utilise des dispositifs d'écoute électronique. Néanmoins, la Cour a aussi déclaré clairement que, pour que les Canadiens puissent être bien protégés contre des abus de ce genre, le Parlement doit renforcer les dispositions du *Code criminel* sur l'écoute électronique.

Le Commissaire à la protection de la vie privée se voit donc forcé de presser le gouvernement de proposer - et le Parlement de promulguer - les mesures nécessaires pour assurer un contrôle adéquat des pratiques de surveillance électronique.

Cela dit, la fiche de protection de la «vie privée» de la Cour suprême ne finit pas cette année en queue de poisson, tout au contraire : elle se termine par un coup d'éclat, avec la décision rendue dans *Santiago Wong c. La Reine* (22 novembre 1990).

L'arrêt *Wong* est le point d'aboutissement d'une enquête sur une maison de jeu menée par la police de Toronto à l'été de 1984. Les responsables de la sécurité d'un important hôtel du centre de Toronto avaient informé la police qu'ils soupçonnaient que des clients tenaient une maison de jeu à l'hôtel. On avait trouvé des indices dans une chambre d'hôtel qu'un client venait de libérer; la police avait appris que la personne qui avait réservé cette chambre, M. Wong, l'avait aussi réservée pour un autre jour, le même mois.

La police avait donc décidé d'installer une caméra vidéo dans la chambre, avec la permission de la direction de l'hôtel, mais sans autorisation judiciaire ni mandat. Les activités qui se sont ensuites déroulées dans la chambre ont été surveillées en cinq occasions, par suite de quoi M. Wong et dix autres personnes ont été accusés d'avoir tenu une maison de jeu.

Le juge de première instance avait conclu que la surveillance magnétoscopique était une violation de l'article 8 de la *Charte*, et il avait rejeté toutes les accusations. La Cour d'appel de l'Ontario avait toutefois jugé que les invitations à se rendre dans la chambre avaient été largement diffusées dans la communauté chinoise de Toronto, et que l'occupant de la chambre y avait reçu de purs inconnus. Compte tenu de ces faits, la Cour d'appel avait conclu que l'accusé ne pouvait pas raisonnablement s'attendre à ce qu'on respecte sa vie privée et que, par conséquent, l'article 8 de la *Charte* ne s'appliquait pas en l'espèce. Elle avait ordonné la tenue d'un nouveau procès.

Les opinions dissidentes de M. le juge La Forest et de M^{me} la juge Wilson font ressortir les lacunes de l'opinion de la majorité. Les deux ont en effet déclaré que, puisque la surveillance électronique des téléphones publics donne lieu, par sa nature même, à d'importantes violations de la vie privée, les autorisations judiciaires requises doivent être expresses et non implicites, comme dans le cas de la clause générale des «endroits fréquentés». Faut-il se prononcer en ce sens, la Cour suprême a laissé au Parlement le soin de s'assurer que la police ne violera pas la *Charte*. Ainsi, les rôles respectifs de la *Charte* et du Parlement ont été inversés. Le juge La Forest l'a déclaré avec éloquence:

Il est évident que la Loi (*Code criminel*) et la *Charte* imposent aux tribunaux une lourde obligation de protéger la vie privée des Canadiens. La surveillance électronique est systématiquement acquiescitive; sa portée vise les conversations tant des innocents que des coupables. La nature systématiquement acquiescitive de la surveillance électronique incite les tribunaux à redoubler de vigilance et à être particulièrement conscients des risques que certaines pratiques minent l'attente des Canadiens en matière d'inviolabilité de leurs communications privées. Cette attente légitime et raisonnable en matière de vie privée ne survivra pas longtemps si les tribunaux accordent leur *imprimatur* à des pratiques qui permettent aux policiers d'intercepter des communications privées pour la seule raison qu'ils ont des motifs raisonnables de croire que de précieux éléments de preuve peuvent ainsi être obtenus. À mon avis, les

clauses des «endroits fréquentés» peuvent facilement entraîner l'application de cette norme peu élevée et constituent des «recherches à l'aveuglette très étendues» dénoncées par notre Cour dans l'arrêt *Hunter c. Southam*, précité à la p. 167. Il est triste de penser que, même avec l'aide de la *Charte*, les tribunaux n'ont pas pris les mesures nécessaires pour prévenir ce danger et que si les Canadiens doivent être protégés adéquatement contre la menace insidieuse que la surveillance électronique pose à la vie privée, ils doivent se tourner vers le Parlement pour obtenir des garanties supplémentaires. Il y a une ironie cinglante dans tout cela. La *Charte* est destinée à nous protéger contre toute possibilité d'empiètement par le Parlement sur les droits individuels.

(p. 14)

Par conséquent, l'arrêt *Thompson* ne peut guère inspirer au Commissaire que des sentiments mitigés. Nous devons applaudir quand la Cour suprême insiste - et c'est nouveau - pour que le droit à la vie privée des innocents soit protégé lorsque la police intercepte des communications privées. En outre, la Cour invite clairement les juges et la police à faire preuve d'une extrême prudence dans les cas où des dispositifs d'écoute sont installés dans des endroits fréquentés par le public. Bien que la Cour n'en fasse pas une obligation, elle recommande en outre que l'écoute électronique soit doublée d'une surveillance visuelle, pour faire en sorte que seules les conversations des suspects soient interceptées. Les Canadiens devraient être réconfortés de constater que la Cour suprême est consciente des risques que la vie privée

La Cour d'appel de la Colombie-Britannique n'avait pas été du même avis; elle avait renversé la décision rendue en première instance et ordonné la tenue d'un nouveau procès. Dans sa conclusion, elle avait déclaré qu'il n'était pas nécessaire que l'autorisation fût expressément mention de téléphones payants, pourvu que la surveillance de ces téléphones n'ait pas été systématique. Pour la Cour d'appel, la communication interceptée en elle-même pouvait prouver que la surveillance téléphonique n'avait pas été systématique, du moment qu'on pouvait y entendre la voix d'un suspect.

La Cour suprême du Canada a tranché la question à la majorité (à quatre contre deux), dans *Thompson et autres c. La Reine*. Cet arrêt rendu public le 18 octobre 1990 est extrêmement intéressant, mais plutôt curieux. Dans les motifs de jugement de la majorité, le juge Sopinka a conclu que la clause générale d'autorisation était légale, même si elle ne faisait aucune mention des téléphones publics et ne prévoyait rien pour la protection du public. Toutefois, il s'est demandé si les interceptions - dûment autorisées - étaient «raisonnables», conformément à l'article 8 de la *Charte*.

Le juge Sopinka a conclu que, dans au moins quatre cas, on avait placé des dispositifs d'interception sur des téléphones publics simplement parce que ceux-ci étaient situés près de l'endroit où demeurerait l'un des suspects. Selon lui, ce n'était pas là une preuve suffisante pour agir, car elle n'équivalait «... à rien de plus qu'une surveillance systématique fondée sur une intuition» (p. 27). En outre, comme l'écoute risquait de porter atteinte à la vie privée de personnes innocentes (des centaines de conversations privées auxquelles aucun des suspects ne participait ont pu être interceptées), le juge a conclu que la surveillance constituait une infraction à l'article 8 de la *Charte*.

Venons-en maintenant à l'aspect curieux de cet arrêt. Le juge Sopinka a déclaré que l'utilisation de la preuve obtenue grâce à la surveillance électronique de téléphones publics ne risquait pas de discréditer l'administration de la justice. Il a donc rejeté l'appel et ordonné la tenue d'un nouveau procès.

Qu'y a-t-il de réconfortant à cela? La Cour suprême fait une mise en garde explicite contre les clauses générales autorisant l'utilisation de dispositifs d'écoute. Elle recommande fortement aux juges et à la police de réduire au minimum les risques d'intrusion dans la vie privée des personnes innocentes lorsqu'il est question d'autoriser l'utilisation de dispositifs d'écoute ou d'obtenir une telle autorisation et d'intercepter des communications. Et pourtant, la police se fait somme toute dire que, même si elle ne respecte pas les normes, elle pourra se servir de ce qu'elle aura découvert contre les suspects.

Pour le Commissaire à la protection de la vie privée, il est à la fois fascinant et encourageant de voir la Cour suprême du Canada accorder une si grande place au droit à la vie privée dans le contexte de la *Charte canadienne des droits et libertés*. C'est fascinant, puisqu'il y a des hauts et des bas, et encourageant aussi parce que, dans l'ensemble, le droit à la vie privée se renforce.

Il a déjà été question de ce dossier passionnant dans deux rapports annuels antérieurs. Cette année, il y a plus encore à dire.

Le 1^{er} septembre 1983, la police avait saisi 278 livres de marijuana dans un véhicule et accusé plusieurs personnes de conspiration en vue de l'importation d'une substance illégale. L'accusation était fondée sur les enregistrements de 136 appels téléphoniques interceptés au cours d'une enquête poussée dans des localités de la Colombie-Britannique très éloignées les unes des autres.

La police croyait que les complices communiquaient en utilisant des téléphones publics payants. Elle avait donc installé des dispositifs d'écoute sur vingt de ces téléphones, qui avaient été reliés à des enregistreuses à quelque vingt reprises, pour enregistrer automatiquement, la nuit durant, les conversations téléphoniques des suspects et d'autres personnes. La police avait bien sûr obtenu des autorisations judiciaires pour installer des appareils d'écoute sur des téléphones, mais jamais expressément sur des téléphones publics. Plus exactement, les autorisations comportaient une clause générale permettant à la police d'intercepter des communications à certaines adresses et "...à d'autres endroits de la Colombie-Britannique fréquentés par (les suspects)..."

Le juge de première instance avait conclu que les autorisations judiciaires étaient invalides, car, à moins d'avoir été expressément autorisé par un juge, l'enregistrement automatique des conversations faites à des téléphones publics payants équivaut à du ratiassage, ce que le *Code criminel* ne permet pas. Le juge avait donc considéré les communications interceptées comme inadmissibles en preuve et il avait enjoint au jury d'acquitter les accusés.

L'année du Commissariat

Comme presque chaque année depuis la création du Commissariat, le nombre de plaintes, d'enquêtes et de vérifications a augmenté. Les détails sont présentés dans d'autres chapitres du rapport, mais un fait demeure : le Commissariat fonctionne à plein rendement, et, nonobstant les restrictions globales d'aujourd'hui, les députés et sénateurs doivent bien se rendre compte que les obligations qu'ils lui ont imposées aux fins de l'application de la Loi sur la protection des renseignements personnels ne peuvent continuer d'être assumées de façon efficiente qu'au prix d'une modeste augmentation de l'effectif actuel de 34 personnes. En effet, nous traitons aujourd'hui plus de 1 200 plaintes par année, soit plus de 160 par enquêteur. L'expérience nous a appris que nous n'échapperons pas à une importante augmentation de cette charge de travail, mais cette augmentation nous forcera à réduire la qualité du service.

La Direction de l'observation a aussi été très occupée. Il faut toutefois souligner qu'en huit ans d'activité, elle n'a pu faire des vérifications que dans environ le cinquième des 150 ministères et organismes fédéraux assujettis à la Loi sur la protection des renseignements personnels. Il est donc bien évident que, si l'on veut élargir la portée de la Loi et charger la Direction de faire des vérifications dans le secteur privé, son effectif de neuf personnes ne suffira pas à la tâche.

Dans le domaine de la recherche, le Commissariat a concentré ses efforts de la dernière année sur une étude des implications du dépistage des drogues en matière de protection de la vie privée. Ses travaux l'ont amené à conclure que les tests de dépistage obligatoires au hasard administrés par l'employeur sont injustifiés, voire, dans certaines circonstances, probablement illégaux. Le Commissariat a été heureux de constater que Transports Canada a modifié dans une certaine mesure ses projets de dépistage des drogues, mais il est très déçu de voir que le ministère de la Défense nationale et au moins une banque à charte vont adopter des programmes de dépistage qui constituent des violations injustifiées de la vie privée de leur personnel. (Cette question est analysée de façon plus détaillée dans un autre chapitre du rapport.)

Enfin, nous mettons la dernière main à un rapport sur les répercussions des progrès de la recherche et du dépistage génétique, qui constitue de toute évidence une plus grande menace pour la vie privée que le dépistage des drogues. Ce rapport devrait être publié à la fin de l'été 1991.

Par contre, il est bien établi dans la fonction publique que des subordonnés consultent, commentent et même contestent, s'ils le désirent, les évaluations de leur rendement faites par leurs supérieurs.

Cela dit, il est dangereux et tout à fait injustifié de prétendre qu'on peut contourner le droit à la vie privée en confiant ces évaluations inversées à des contractuels. Si c'était possible, l'administration fédérale pourrait se soustraire à tous ses objectifs de protection de la vie privée en confiant toute la gestion des renseignements personnels à l'entreprise privée. Les risques sont énormes et vont bien au-delà de ce que les cadres risqueraient s'ils perdaient leur droit d'accès à l'information qui les concerne et du fait que la Loi ne protégerait plus des renseignements aussi personnels d'une utilisation ou d'une divulgation abusives. Il reste que, une fois le marché conclu, les contractuels sont des agents de l'administration fédérale, et que celle-ci conserve donc le « contrôle » des renseignements en question où qu'ils soient conservés.

Bien peu de gens contestent le désir du gouvernement d'améliorer la gestion et l'imputabilité de l'administration fédérale, mais il fait sûrement fausse route en choisissant pour le faire un procédé qui saperait sa propre législation.

Pour ce genre d'évaluation, le subalterne remplit un questionnaire en cotant son supérieur en fonction de ses aptitudes de gestion et de ses traits personnels. Les questionnaires remplis sont ensuite analysés, parfois par un contractuel, et leur contenu est résumé. Les cadres reçoivent un exemplaire du rapport qui en résulte, mais ils n'ont pas accès aux cotes ou aux commentaires de leurs subordonnés.

Néanmoins, le nouvel outil de gestion que les ministères et organismes adoptent avec enthousiasme, l'évaluation inversée (ou si l'on préfère de bas en haut) présente une grande partie des mêmes dangers pour notre vie privée. Comme le terme l'implique, c'est un procédé qui permet aux subalternes d'évaluer - anonymement - le rendement de leurs supérieurs. Jusqu'à présent, il a été utilisé dans de grandes entreprises privées, mais il est tout nouveau pour les institutions gouvernementales, qui refondent actuellement leurs systèmes d'évaluation du rendement dans le contexte de la réforme globale de la fonction publique.

Le procédé soulève plusieurs difficultés en matière de protection de la vie privée, la première étant, bien entendu, le fait qu'on promet aux « évaluateurs » que les renseignements fournis seront traités de façon confidentielle pour leur éviter des représailles. En effet, la Loi sur la protection des renseignements personnels donne à chacun le droit de savoir ce qu'on dit ou ce qu'on écrit à son sujet. Par conséquent, si l'on promet à ceux qui font les évaluations que celles-ci seront traitées de façon confidentielle, on les induit en erreur, car cette promesse est illégale.

les renonciations qu'on leur demandait de signer et ils en ont informé le Commissariat, mais nous craignons que la plupart n'y aient vu que du feu. Des dispositions contractuelles comme celles-là, imprimées en petits caractères, ne satisfont absolument pas aux exigences d'obtention d'un consentement en toute connaissance de cause. Qui plus est, elles ne reflètent pas l'attitude de respect accru de la vie privée dont l'Association des banques à charte se réclame désormais.

Cela dit, il y a eu des progrès. Nous devons notamment féliciter l'Association canadienne du marketing direct, qui a adopté une méthode grâce à laquelle les consommateurs peuvent faire rayer leur nom des listes d'expédition de leurs membres.

C'est un pas en avant, parce que l'Association regroupe environ 80 p. 100 des entreprises faisant du marketing direct.

Il reste que des améliorations aussi modestes sont bien insuffisantes face à l'explosion du volume des échanges de renseignements rendus possibles par l'ordinateur. C'est pourquoi le strict minimum en matière de normalisation des échanges de renseignements personnels doit être l'introduction de codes dument approuvés pour toutes les entreprises de compétence fédérale. Pour le Commissaire, c'est urgent.

Evaluation des gestionnaires

Nous recommandons aussi au Parlement de prendre des mesures pour rétablir la protection des communications téléphoniques personnelles au Canada, qui tend à s'éroder en raison de la prolifération des téléphones cellulaires. En effet, ces communications électroniques risquent d'être aisément interceptées par de l'équipement qu'on peut se procurer facilement, et elles le sont effectivement. L'absence de fils téléphoniques ordinaires ne devrait pas priver les usagers du téléphone du droit à leur vie privée et du droit de s'attendre à ce que leur intimité soit protégée. La vente ou la possession d'équipement de surveillance devrait être interdite, sauf dans le cas des organismes autorisés à s'en servir conformément à la législation qui régit ce genre d'activités.

Cela dit, même si les codes d'autoréglementation deviennent chose courante sur le marché canadien, seront-ils vraiment efficaces? Des spécialistes très respectés restent convaincus qu'un contrôle s'impose avant que l'entreprise privée soit en mesure de rendre des comptes au public sur ses activités de protection de la vie privée.

Le professeur David Flaherty, l'universitaire canadien le plus réputé en matière de recherche sur la protection de la vie privée, soutient que l'administration fédérale doit pouvoir faire des vérifications pour que le secteur privé respecte ses propres codes d'autoréglementation. Son opinion pèse lourd dans la balance, mais le Commissaire continue à croire, à l'instar de son prédécesseur, qu'une intervention d'une telle ampleur - avec les ressources énormes qu'elle nécessiterait - ne devrait avoir lieu qu'en dernier recours, si l'on prouve hors de tout doute que le secteur privé ne peut pas ou ne veut pas s'autoréglementer.

Il reste manifestement bien du chemin à faire jusque là. Nous ne citerons qu'un petit exemple : dans leurs demandes de cartes de crédit, certaines banques à charte réclament encore - en petits caractères - une renonciation de leurs clients à tous leurs droits à la vie privée. Ces renonciations donnent aux banques le droit de réutiliser à leur gré tout ou partie des renseignements que leurs clients leur fournissent, notamment sur leur traitement ou leur salaire, leurs antécédents professionnels et leurs biens, ainsi que, dans un cas, leur numéro d'assurance sociale. Quelques consommateurs alertes ont remarqué

C'est sans doute en réponse à une inquiétude croissante des consommateurs que le secteur privé semble commencer à prendre des mesures encourageantes. Certains diront sûrement qu'il est plus que temps, mais il reste que l'Association des banquiers canadiens, Bell Canada et l'Association canadienne du marketing direct se sont donné l'an dernier des codes d'éthique qui amélioreront sensiblement la protection des renseignements personnels et confidentiels concernant leurs clients. Nous vous en parlerons davantage plus loin, mais il vaut la peine de préciser dès maintenant que ces mesures d'autoréglementation ont des possibilités.

En fait, il ne s'agit pas tant de savoir si le secteur privé peut continuer à se passer de codes de protection des renseignements personnels, mais plutôt combien de temps il pourra le faire avant qu'on lui impose des règles. Les événements récemment survenus en Europe empêcheront peut-être bientôt les entreprises nord-américaines de se livrer à des transferts de données avec leurs homologues européennes à moins d'avoir des codes de ce genre. Cette évolution rend plus urgente encore la recommandation que le Commissaire avait adressée au Parlement l'an dernier, en demandant que la *Loi sur la protection des renseignements personnels* soit modifiée de façon à obliger toutes les entreprises privées de compétence fédérale à adopter des codes de protection des renseignements personnels fondés sur des règles et des principes internationalement reconnus.

Et pourtant, si nous partons du principe que la vie privée ne peut avoir de meilleur défenseur qu'un public bien informé et désireux d'agir, l'année écoulée laisse entrevoir des indices très encourageants de gains réels et durables.

Dans le secteur privé

Les rapports annuels antérieurs ont fait état d'une sensibilisation croissante du public aux méthodes de marketing invasives du secteur privé. En 1990, cette question a même reçu la suprême accolade médiatique, la Une du TIME. En outre, et même si certains des participants auraient peut-être voulu échapper à cette publicité, une autre preuve de l'importance accrue que l'opinion publique accorde à la protection de la vie privée nous est venue de l'arène politique dans deux provinces où des ministres ont éprouvé de telles difficultés par suite de divulgations de renseignements personnels que l'un d'eux a dû démissionner. Quoi qu'on puisse en penser, ces événements montrent bien qu'on ne peut pas toujours faire fi impunément du droit à la vie privée. En fait, si le marché a été ces dernières années la source de certaines des pires menaces pour notre intimité, il se peut fort bien qu'il finisse par s'autocorriger, au moins en partie dans son propre intérêt.

À la lecture des rapports annuels antérieurs, on ne manque pas d'être frappé par ce phénomène. Bien des questions qui dominent la discussion aujourd'hui faisaient à peine partie de notre lexique il y a tout juste huit ans. De nos jours, nous parlons énormément de dépistage des drogues et du SIDA, ainsi que des implications de la recherche juridique et de l'interception des communications par téléphone cellulaire, pour ne citer que quelques exemples, et nous reviendrons d'ailleurs sur certains d'entre eux plus loin. Il est certain que cette tendance se maintiendra, car rien ne laisse entrevoir le moindre ralentissement du progrès des sciences et de la technologie. Le mieux que nous puissions faire, c'est monter la garde pour être prêts à endiguer les attaques contre la vie privée, en tentant de réparer les brèches au fur et à mesure et en n'étant sûrs de rien, sauf que la lutte se poursuivra indéfiniment.

Cela dit, comment les choses se sont-elles passées au cours de la dernière année?

En bien, rien ne nous permet de croire que la vague technologique qui sape notre intimité soit en voie de s'apaiser. Les ordinateurs continuent à proliférer (l'administration fédérale à elle seule en aurait 80 000, selon les dernières estimations); le courrier non sollicité continue à s'accumuler; le commerce des renseignements personnels prend de plus en plus d'ampleur (son chiffre d'affaires annuel atteint les 3 milliards de dollars aux États-Unis, ce qui correspond probablement à 300 millions de dollars au Canada).

S'il a jamais existé, le droit qu'on nous laisse tranquille ne subsiste plus que dans les coins les plus reculés de l'Arctique, et encore... En effet, il y a gros à parier que nos ermites verront bientôt apparaître à l'horizon des fonctionnaires intrépides porteurs de la formule suprême qui, dûment remplie, leur confèrera le certificat irrefutable d'appartenance à l'espèce humaine, un numéro d'assurance sociale.

Bref, dans notre société moderne, il est impossible de protéger complètement son intimité; ce n'est d'ailleurs ni pratique, ni même particulièrement désirable, mais nous continuerons à lutter pour préserver le droit de chacun de déterminer jusqu'à quel point sa vie privée doit être sacrifiée à d'autres droits.

C'est pour cette raison que l'idée d'un tableau annuel de la situation risque d'être trompeuse, si utile qu'elle soit pour évaluer les résultats, à moins que nous ne comprenions clairement qu'en matière de protection de la vie privée, les citoyens sont toujours en danger, étant donné qu'ils subiront immanquablement de nouvelles attaques dès qu'on aura trouvé la parade aux anciennes.

Dans le rapport de cette année, tout comme dans ceux des années précédentes, nous tenterons de brosser un tableau réaliste de la situation de la protection de la vie privée au Canada, c'est-à-dire de donner et les bonnes, et les mauvaises nouvelles. Dans un domaine comme celui-là, la victoire n'est jamais acquise. En effet, la protection de la vie privée est si intimement liée à la relation entre l'individu et la société que l'évolution du tissu social se répercutera toujours sur la vie privée des citoyens.

Contrairement à ce que certains cyniques prétendent, ce n'est pas un droit invoqué seulement par ceux qui ont quelque chose à cacher, car si nos libertés d'expression fondamentales ne sont pas protégées par un certain respect de notre intimité, il ne sera plus possible d'avoir des idées, des amis et des connaissances.

En 1898, lorsqu'il a donné une définition restée célèbre du droit à la vie privée (le droit qu'on nous laisse tranquille), le juge Brandeis n'aurait jamais imaginé un monde de machines ingénieuses dotées d'une capacité illimitée pour collecter, colliger et transmettre des renseignements dans des réseaux planétaires, pas plus d'ailleurs qu'une science capable de sonder les arcanes les plus secrètes de l'hérédité de l'être humain.

Il s'est écoulé une dizaine de mois entre le départ de l'ancien Commissaire et la confirmation du nouveau. Pendant cette période, le directeur général, Alan Leadbeater, a assumé à titre intérimaire les fonctions de commissaire, en jouant un double rôle difficile, celui de directeur administratif et d'ombudsman. Sous certains aspects, le nouveau Commissaire, qui est entré en fonction presque à la veille du dépôt du rapport, est le porte-parole de ses deux

prédécesseurs, qui l'ont fait bénéficier de leurs conseils et de leur expérience pendant qu'il était commissaire adjoint. Les dix mois qu'il a passés à ce poste ont été pour lui une période inestimable d'introduction à un domaine dont la complexité déjà grande s'accroît sans cesse. Si le lecteur décèle un certain manque d'assurance dans le ton du rapport, il n'aura pas tort de l'imputer au fait que son auteur sait qu'il a encore beaucoup à apprendre.

Qu'à cela ne tienne, il n'est pas le seul! En effet, la relève de la garde s'est faite aussi au Québec et en Ontario cette année. Paul-André Comeau est devenu le nouveau Commissaire à l'information et à la protection de la vie privée du Québec, et Thomas Wright a assumé les mêmes fonctions en Ontario. Bref, les titulaires ont changé, mais la relation de cordialité et d'aide mutuelle des trois Commissariats, elle, devrait se maintenir sans difficulté.

Ce rapport annuel du Commissaire à la protection de la vie privée est le premier en huit ans à ne pas être soumis au Parlement par John Grace. Jusque'en juin 1990, M. Grace a été le seul Commissaire à la protection de la vie privée que le Canada ait connu, depuis 1983, quand sa fonction est devenue distincte de celle du Commissaire aux droits de la personne.

M. Grace a quitté le Commissariat avec une réputation remarquable à de nombreux égards, d'abord parce qu'il a été un ombudsman doué d'un talent exceptionnel pour régler des problèmes et des plaintes en matière de vie privée, puis parce qu'il a su être un apôtre énergique et éloquent de la protection de la vie privée et enfin parce qu'il a été le chef respecté d'un petit groupe d'enquêteurs et de vérificateurs très motivés, auquel il a communiqué son engagement indéfectible pour ce secteur aussi vital que menacé des droits de la personne.

En outre, M. Grace a toujours été sensible aux défis qui continuent d'être jetés en si grand nombre - et à une vitesse vertigineuse - aux défenseurs de la vie privée, dans un environnement commercial et technologique toujours changeant.

Bref, John Grace a légué à son successeur une organisation bien rodée.

Une grande partie des questions qui figurent dans ce rapport annuel ont été abordées avant le départ de M. Grace.

La Loi sur la protection des renseignements personnels donne aux individus accès à leurs renseignements personnels détenus par le gouvernement fédéral; protège la vie privée des individus en restreignant le nombre des personnes qui peuvent consulter les renseignements; et donne aux individus un certain contrôle sur la collecte et l'usage des renseignements par le gouvernement.

La Loi énonce les principes des pratiques équitables en matière d'information qui exigent que le gouvernement:

- ne collecte que les renseignements dont il a besoin pour exécuter ses programmes;
 - recueille les renseignements directement auprès de l'individu concerné, dans la mesure du possible;
 - informe l'individu des fins auxquelles ils sont destinés;
 - conserve les renseignements suffisamment longtemps pour en assurer l'accès aux individus; et
 - veille « dans la mesure du possible » à ce que les renseignements personnels soient exacts et complets.
- Toute personne présente au Canada peut déposer une plainte auprès du Commissaire à la protection de la vie privée si:
- elle s'est vu refuser une partie quelconque des renseignements;
 - le droit de demander la correction de certains des renseignements contenus dans le fichier ou de les annoter leur est refusé;

- le ministère prend plus des 30 jours initiaux ou des 60 jours maximums pour fournir les renseignements;
- la description du contenu des fichiers de renseignements donnée dans le manuel *Info Source* est incorrecte à un quelconque égard;
- la liste donnée dans ce manuel pour chaque ministère ne décrit pas tous les usages qui sont faits des renseignements personnels;
- une institution recueille, conserve, utilise ou élimine des renseignements personnels d'une manière qui contrevient à la *Loi sur la protection des renseignements personnels*.

Les enquêteurs du Commissariat à la protection de la vie privée examinent tous les fichiers (y compris ceux considérés inconsultables), à l'exception des renseignements confidentiels du Conseil privé de la Reine, pour s'assurer que les institutions fédérales se conforment à la Loi.

La Loi confère également au Commissaire à la protection de la vie privée le pouvoir de vérifier la façon dont les institutions fédérales recueillent, utilisent et éliminent les renseignements personnels, sans devoir attendre qu'une plainte soit déposée.

Mandat.....	1
Le chef d'orchestre change, pas le refrain.....	2
La protection de la vie privée et la Charte.....	9
Les téléphones cellulaires et la protection de la vie privée.....	15
La protection de la vie privée dans le secteur privé.....	18
Tests biomédicaux.....	22
La réforme électorale - une liste électorale permanente.....	26
La protection de la vie privée et l'intérêt public: un équilibre difficile à protéger.....	28
Direction des plaintes.....	31
Rapport de la Direction.....	31
Tableaux et graphiques.....	35
Dossiers.....	40
Aviser le Commissaire.....	51
Politique et recherche.....	55
Couplage de données.....	55
La technologie continue à progresser.....	62
Consultation auprès du Commissaire.....	65
Demandes de renseignements.....	68
Direction de l'observation.....	70
Gestion intégrée.....	75
Organigramme.....	77

L'honorable John A. Fraser, c.p., c.r., député
Président
Chambre des communes
Ottawa

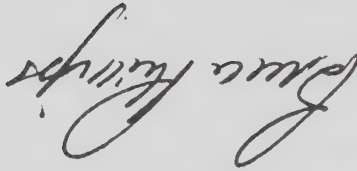
le 28 juin 1991

Monsieur Fraser,

J'ai l'honneur de soumettre mon rapport annuel au Parlement. Ce rapport couvre la période allant du 1^{er} avril 1990 au 31 mars 1991.

Vous en agréer l'expression de mes sentiments respectueux.

Le Commissaire à la protection de la vie privée



Bruce Phillips

L'honorable Guy Charbonneau
Président
Sénat
Ottawa

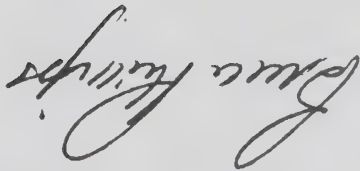
le 28 juin 1991

Monsieur Charbonneau,

J'ai l'honneur de soumettre mon rapport annuel au Parlement. Ce rapport couvre la période allant du 1^{er} avril 1990 au 31 mars 1991.

Veuillez agréer l'expression de mes sentiments respectueux.

Le Commissaire à la protection de la vie privée



Bruce Phillips

Le Commissaire à la protection de la vie privée du Canada
112, rue Kent,
Ottawa (Ontario)
K1A 1H3

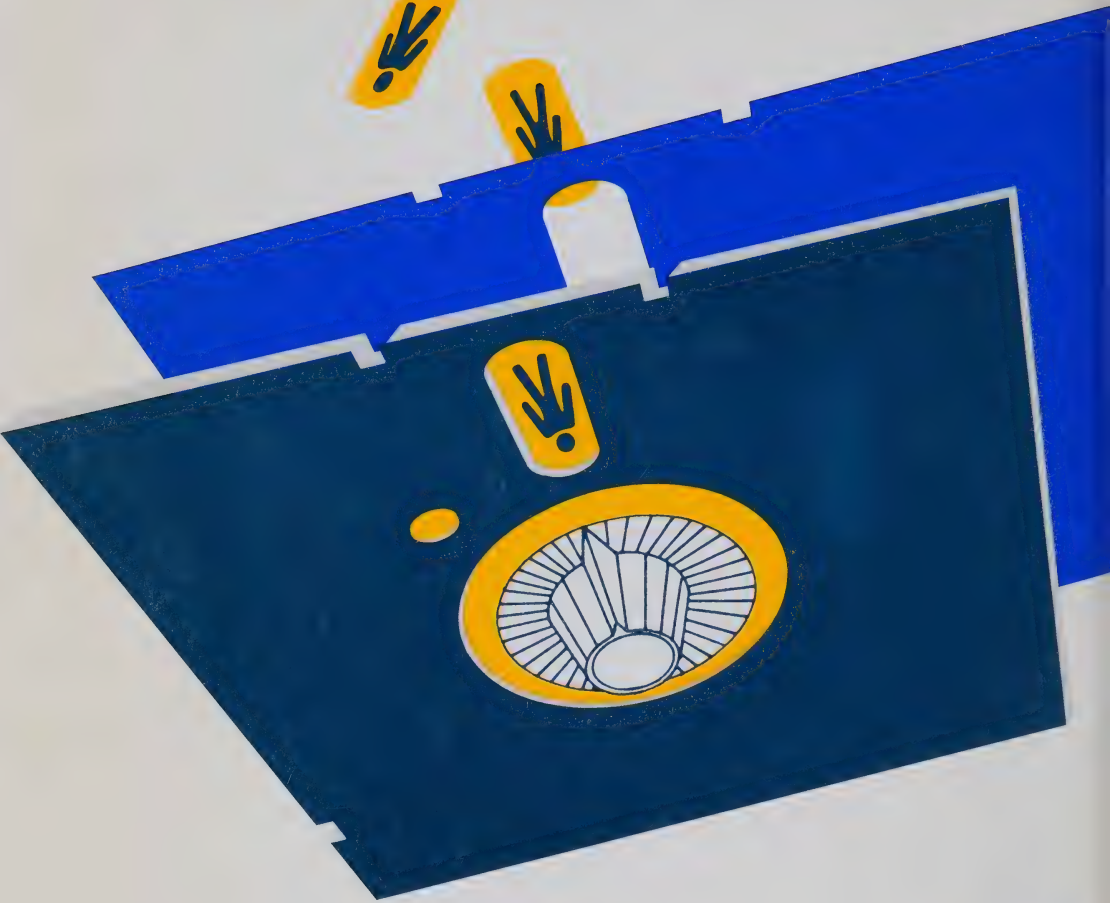
(613) 995-2410, 1-800-267-0441
Télec. (613) 995-1501

© Ministre des Approvisionnement et Services Canada 1991
N° de cat. IP30-1/1991

ISBN 0-662-58483-X

**Rapport annuel du
Commissaire à la protection de la vie privée
1990-91**





Commissionnaire à la
protection de la vie privée
Rapport annuel 1990-1991

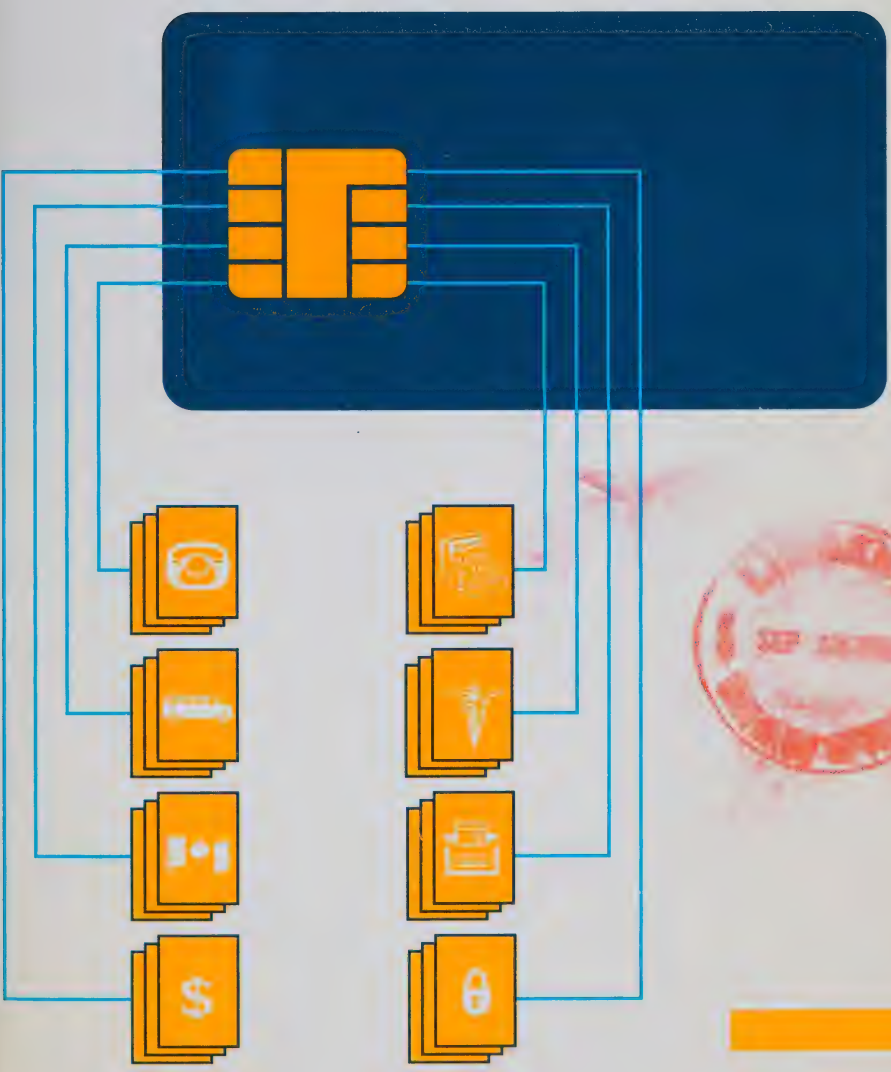


CAI
PC
-AST



Privacy Commissioner

Annual Report 1991 - 92



**Annual Report
Privacy Commissioner
1991-92**



Front Cover: The new "smart cards" look like bank or credit cards but there is an essential difference. Imbedded in the card is a computer chip to process and store data and to identify the owner. The symbols illustrate the range of services and personal information that may soon be stored on one small piece of plastic. They are:

- | | |
|--------------------------|----------------------------------|
| ■ Telephone calling card | ■ Retail purchases |
| ■ Bus pass | ■ Medical records |
| ■ Federal benefits | ■ Computer system access |
| ■ Banking services | ■ Residence and workplace access |

The Privacy Commissioner of Canada
112 Kent Street
Ottawa, Ontario
K1A 1H3

(613) 995-2410, 1-800-267-0441
Fax (613) 995-1501
TDD (613) 992-9190

© Minister of Supply and Services Canada 1992

Cat. No. IP30-1/1992

ISBN 0-662-59183-6

The Honourable Guy Charbonneau
The Speaker
The Senate
Ottawa

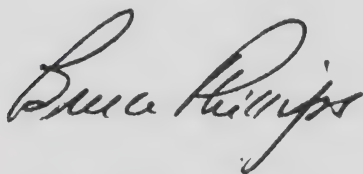
August 12, 1992

Dear Mr. Charbonneau:

I have the honour to submit to Parliament my annual report.

This report covers the period from April 1, 1991 to March 31, 1992.

Yours sincerely,

A handwritten signature in dark ink, appearing to read "Bruce Phillips". The signature is fluid and cursive, with the first name "Bruce" and the last name "Phillips" clearly distinguishable.

Bruce Phillips
Privacy Commissioner

The Honourable John Fraser, P.C., Q.C., M.P.
The Speaker
The House of Commons
Ottawa

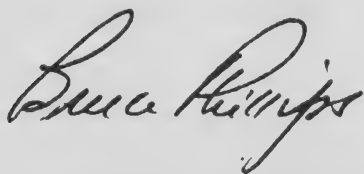
August 12, 1992

Dear Mr. Fraser:

I have the honour to submit to Parliament my annual report.

This report covers the period from April 1, 1991 to March 31, 1992.

Yours sincerely,

A handwritten signature in dark ink, reading "Bruce Phillips". The signature is written in a cursive, flowing style with a large initial "B".

Bruce Phillips
Privacy Commissioner

Table of Contents

Mandate	1
The End of the Beginning?	3
Charter privacy protection	8
Privacy in banking and telecommunications	10
The private sector: voluntary action	12
Privacy at work	14
Fine tuning the Act.....	15
Redefining "personal information"	16
Tightening up disclosures	17
Broadening the injury test	19
"Catch 22"	21
Genetic Testing and Privacy.....	23
A Year in the Privacy Trenches	27
Telecommunications toys—playing with privacy..	27
This year's SINs	31
Technology update.....	34
Data matching.....	38
Complaints Directorate	41
Some cases	52
Notifying the Commissioner	64
Inquiries—the public talks back.....	70
Compliance Directorate.....	75
Trends and problems	75
Contracting out—who's minding the data?	76
Checking employee credit ratings	77
Electronic transmission of personal information ..	78
Who's minding the computer?	79
Upward appraisals	82
Corporate Management Branch	83
Organization Chart.....	86

Mandate

The *Privacy Act* provides individuals with access to their personal information held by the federal government; it protects individuals' privacy by limiting those who may see the information; and it gives individuals some control over the government's collection and use of the information.

The Act sets out the principles of fair information practices, requiring government to :

- collect only the information needed to operate its programs;
- collect the information directly from the individual concerned, whenever possible;
- tell the individual how it will be used;
- keep the information long enough to ensure an individual access; and
- “take all reasonable steps” to ensure its accuracy and completeness.

Anyone in Canada may complain to the Privacy Commissioner if:

- they are denied any part of the information;
- they are denied their request to correct some of the information on the file — or their right to annotate it;
- the department takes longer than the initial 30 days or maximum 60 days to provide the information;
- the *Info Source* description of the contents of an information bank is deficient in some way;
- the department's listing in the Source does not describe all the uses it makes of personal information;

-
- an institution is collecting, keeping, using or disposing of personal information in a way which contravenes the *Privacy Act*.

The Privacy Commissioner's investigators examine any file (including those in closed banks) except confidences of the Queen's Privy Council to ensure that government institutions are complying with the Act.

The Act also gives the Privacy Commissioner the power to audit the way government institutions are collecting, using and disposing of personal information.

The End of the Beginning?

It may be tempting fate beyond prudent limits. Nevertheless, with crystal ball and reputation in hand, the author is willing to venture the opinion that the privacy picture is getting a little better.

Not yet the sunlit uplands, to be sure: disaster areas abound, and the rubble of many a previous privacy defeat remains untouched.

But, carrying Churchillian paraphrase to unreasonable limits, one senses that, while we are a long way from the beginning of the end to privacy problems, we may be close to the end of the beginning.

In plain talk, we seem to be getting somewhere.

During the year under review, there were a number of developments on several fronts which suggest the slow-gathering defences of privacy are starting to make themselves felt.

Both inside and outside of government there were hopeful signs of greater recognition of the problems affecting privacy, and a greater willingness to seek remedies. To itemize a few of the more outstanding ones:

- Two more provinces, British Columbia and Saskatchewan, are in the process of creating privacy protection schemes. A third, Alberta, is considering similar action. Inclusion of these three provinces would extend some form of data and privacy protection at provincial levels from Quebec to the Pacific Coast.

- Federal legislative activity in the fields of telecommunications and financial institutions stimulated refreshingly intense focus on their privacy implications, both by the government and in Parliament. Some of the proposed responses, still under study as this report goes to press, could point the way to a breakthrough in the difficult problem of achieving higher levels of privacy protection in the private sector.

- Some of the major players in the commercial field are responding more energetically to the rising level of public concern about the way business handles personal information under its control. Notable in this respect are Canada's direct marketers, who are working on a code of practice which, if adopted, offers promise that those among us who do not wish to receive unsolicited mail and telephonic sales pitches will be provided with a convenient and well-publicized method of avoiding them.

- Though technically not within the year, there was a landmark decision by the Canadian Radio and Telecommunications Commission (CRTC) in the case of "Caller ID". It established a critical precedent by ruling that telephone subscribers who wished to preserve the anonymity of their telephone numbers would not have to pay a special charge. This ruling clearly recognized that in telecommunications, privacy is recognized as a consumer's right, and not merely as a commodity for sale.

Some of these developments will be discussed in more detail later in this report. They do not constitute in any way a comprehensive account of all that has happened in the many areas of life and commerce which had an impact on privacy during the year. They are presented as examples of a hopeful trend. Taken singly or together, they represent something considerably less than dazzling victories, but something considerably more than deadlock.

However, they must be viewed in the context of the larger problem. For example, all the earnest jawboning of privacy advocates so far has had almost no impact on the biggest and most serious privacy issue of all, which is the vast and unregulated traffic in personal information, a business whose monetary value in North America runs into the billions of dollars. A society which casually accepts the existence of dossiers of unknown accuracy in unknown hands on millions of individuals, and with no rights of access and correction, is a society which is recklessly indifferent to preserving that most basic privacy right: the right to some control over what others know about you. Yet this is the situation as it now stands. There is scarcely one among us whose name is not to be found in one, and probably more of those dossiers in the computer banks of the list-makers and the list-marketers.

It is, though, an indifference born largely of ignorance. There is ample and heartening evidence that wherever and whenever the public at large clearly understands the issues and is given an opportunity to influence them, whole armies rise up to mount privacy's barricades, sometimes with dramatic results.

Item: a couple of years ago, a telephone company in the United States asked its subscribers whether they objected to their information in the company files being sold off to other companies. Eight hundred thousand of them so objected, and the idea was dropped. Likewise, a scheme involving one of the major software companies in the United States to market a machine-readable disc containing information on eighty million persons provoked such a storm of controversy that it too was discarded.

Public reaction — often angry — to the explosion of direct marketing illustrates the critical importance of wider knowledge about the issues. While not implying that marketers are devoid of a sense of responsibility, it would be naive not to acknowledge that it is public concern about the means by which these firms acquire their information which is injecting fresh impetus into the industry's efforts to develop an improved privacy code.

Thus greater public understanding of privacy issues in the modern technological context is a desperate necessity. What simpler and more graphic proof is required than our recent experience with cellular telephones?

Many people were surprised to learn from our last annual report that conversations over cellular telephones could be monitored with easily-obtained scanning equipment. The revelation has not lessened the public affection or appetite for these extremely useful inventions, but we're willing to wager it has made many people considerably more sophisticated or guarded in their use of them.

All that was ever missing in the cellular phone revelation was adequate information. Mass media coverage of the observations of this office helped to fill the information gap. But one would never have been created in the first place had industry been required to ensure that its clientele was provided with all the information needed to make informed decisions about the equipment.

The obligation to inform rests upon both the private and public sectors. In the latter area, the only national agency which seeks to maintain an overview of the entire privacy field is the Office of the Privacy Commissioner. It is, therefore, the natural body to play a lead role in the area of public education and communication. Yet it is a fact (which even some parliamentarians are surprised to discover) that the office has no public education mandate. We do what we can, with almost no resources for the purpose, largely through the medium of this report, speeches and conferences as time permits, and of course the attentions of the media.

None of these factors is to be discounted, particularly the last. Yet much more can and should be done. Forgotten, perhaps, is the government's commitment in 1987 to seek a *Privacy Act* amendment to give the office an education mandate. Let us hope this reminder stimulates action.

Over the years, both the incumbent and previous commissioners have discussed the merits or otherwise of extending the reach of the *Privacy Act* to include federally-regulated private businesses such as banks and transportation companies. In the case of the present Commissioner, this option was regarded not as the best thing to be done, but as possibly the only thing that could be done in the face of apparent failure to obtain good privacy protection in the private sector any other way. The urgency of this question is somewhat diluted by the current examination by Parliament of the privacy problems posed by financial and telecommunications legislation. We must await results to determine whether this case-by-case approach is better. But there are distinct advantages in the sectoral approach made possible by the *Bank Act*, in which

privacy rules for specific industries or services could be developed. This approach is now being adopted in the Netherlands. In the case of Canadian banks, both the Canadian Bankers Association and several of its members already have developed privacy codes which with some improvements and modifications, could well form the basis of a set of regulations governing their handling of personal information. The principal element missing from the codes as they now stand is a system of independent oversight and dispute resolution, which the Commissioner feels is essential to ensure compliance and public confidence. In any event, efforts to produce a more alert and informed body politic is a more urgent priority. An informed public is the best defence against abuse. That holds true for privacy as much as it does for democracy as a whole. It is certainly a pre-requisite to any kind of effective defence.

Charter privacy protection

The value of an aware public must also be considered in the context of a nation which still has no constitutional right to privacy. Although there are various laws such as the federal *Privacy Act*, which give citizens some protection in specific areas of information gathering, and although the Supreme Court has defined a privacy right in some cases—principally involving criminal laws—the acceptance of privacy as a basic human right has not yet found its way into our statutes.

This office has sought to correct this oversight by appearing before the Special Joint Committee on a Renewed Canada to urge that a right to privacy be included among its recommendations.

The submission pointed out that a privacy right was included in almost the very first draft proposed by the federal government when it unveiled its *Charter of Rights and Freedoms*, that it is already included in a number of similar documents such as the *Quebec Charter of Rights*, the *Universal Declaration of Human Rights*, the *European Covenant of Human Rights*, and the constitutions of several states of the American union, to name just a few. Moreover, the proposal has already been favorably viewed by the Commons justice committee (in 1987), and had the support of such important Canadian groups as the Canadian Bar Association.

Unfortunately, the proposal did not command majority support of the committee. Although this office of course was not privy to the committee's *in camera* deliberations, we understand some members expressed concern that inclusion of a privacy right might have an adverse impact on other freedoms or rights, such as speech or access to information. It should be pointed out that a privacy right would be subjected to the same test of balancing the private and public well-being that applies to all rights and freedoms now in the *Charter*. The *Charter* expressly directs that these rights are to be exercised in a manner that is reasonable in a free and democratic society, thereby imposing on the courts the duty to seek a balance between competing or conflicting claims.

The fate of this initiative was particularly disappointing in view of the constitutional exhaustion that is likely to ensue when the current round of negotiations concludes, with the dim prospect of re-opening the *Charter* any time soon. All the same, this is unfinished business on the Commissioner's agenda, and the office will continue to press the case.

Privacy in banking and telecommunications

At the federal level, some kind of Great Divide may have been traversed, with the inclusion of language in two important pieces of legislation which makes it possible to accommodate privacy concerns. The first of these is the revised *Bank Act* and associated statutes, which will make possible the cross-ownership of banks, insurance and trust companies. Given the huge holdings of personal information in financial institutions, this office naturally is concerned by the degree to which these data might be shared in future, and to what extent the consent and control by clients and customers will be involved in the process.

The legislation gives the government authority to make regulations covering such personal information exchanges. In April, the Commissioner appeared before the Senate banking committee to urge that Parliament take advantage of this authority and draft such regulations.

The committee evinced considerable degree of interest in this recommendation, and indicated that the Commissioner might be invited to discuss the subject further. At the same time, the Commissioner understands the Department of Finance is also examining the issue.

A telecommunications bill now before Parliament is even more explicit in recognizing protection of privacy as one of its objectives, the first such example known to the Privacy Commissioner apart from the *Privacy Act* itself.

As of this writing, the outcome of these initiatives is still to be determined. However, the Commissioner must record his satisfaction with this evidence of growing understanding of the privacy issue both in the councils of government and in the federal bureaucracy.

In fact, the Commissioner sees in the above developments a possible answer, or the beginnings of an answer, to the oft-debated issue of regulating information practices in the private sector.

Also on the legislative front, the Commissioner notes with great satisfaction the proclamation of Saskatchewan's *Freedom of Information and Protection of Privacy Act* and the intention of the government of British Columbia to proceed with the introduction of similar legislation. B.C. has engaged the services of Professor F. Murray Rankin as principal consultant, thereby ensuring the process will be favored with both enormous commitment and immense knowledge.

The extension of privacy protection to Canada's third most populous province means that more than 60 per cent of Canadians would enjoy the benefits of privacy oversight at the provincial level (joint Quebec and Ontario). The Commissioner is pleased to report that he has had consultations with officials of one other province now considering similar legislation.

All these developments must be regarded in a highly positive light. They constitute hard evidence that governments more and more are recognizing privacy not only as a right to which all citizens are entitled, but one which in the face of increasingly intrusive technology needs to be supported by its own set of laws and regulations.

The Private Sector: Voluntary Action

As previously mentioned, much of the Canadian banking industry now is covered by voluntary privacy codes. Following the promulgation of a model code by the Canadian Bankers Association, a number of the largest chartered banks have developed their own individual codes. While these codes differ in detail, and while they fall short of what the Commissioner would consider ideal, they share one important characteristic—the recognition that clients and customers have a vested interest in the fate of the personal information which they provide to the banks, and are entitled to some measure of consent and control.

As of this writing, for reasons mentioned earlier, these encouraging if less-than-perfect measures may be overtaken by the revised *Bank Act*. Even so, they provide an important starting point in what should be a joint government-industry effort. If *Bank Act* revisions do not occur, the Commissioner remains convinced that while the banks are to be commended for the progress made so far, their codes will still need to be strengthened.

Also heartening are signs of progress in the direct marketing field, which in recent years and as noted earlier has been the target of much public concern and complaint. The Commissioner commented previously and favorably upon a decision by the Canadian Direct Marketing Association to create a system by which Canadians could have their names removed from marketing lists held by the association's member companies. The association continues to work on an expanded code. It is unpublished as of this writing, but it is the fervent hope of the Commissioner that it will enlarge significantly the role of consumers, at least to the extent that prior consent becomes a condition of inclusion on such marketing lists.

Another promising initiative was undertaken during the year by the Canadian Standards Association (CSA) an organization whose primary responsibility is to ensure the safety and reliability of products marketed in Canada. CSA is most familiar to Canadians from its logo on products which conform to industry standards.

Shortly after the Commissioner's last annual report appeared with its news on the European draft privacy directives, the CSA contacted this office to offer a novel suggestion. CSA proposed formation of a committee to develop a model privacy code, one which would serve as a minimum national standard for private sector organizations handling personal information.

The CSA is ideally placed to develop such a code. It is an independent service organization of business, industry, labour, academia and regulators. This new proposal is a natural extension of the organization's involvement in international technology standards and its interest in technology's impact on consumers, business and industry.

A workable model code for the private sector would balance trade and business interests with consumers' inherent right to privacy. It would also demonstrate Canadian industry's commitment to the privacy principles contained in the OECD guidelines—and thus respond to the EC's requirement for “equivalent or adequate” protection.

The CSA code's committee (of which the office is a member) has drafted a proposal and has already received indications of interest and funding from AMEX, Readers' Digest, Bell Canada, Equifax and the federal departments of Consumer and Corporate Affairs and Communications.

If necessary, CSA will hire an experienced consultant to conduct research and work with the committee to develop the code. Once consensus is reached, the code will serve as the foundation, to be supported by various technical standards. It will become the cornerstone of a national compliance framework to help different business sectors establish privacy codes suitable for their particular environments.

The Commissioner strongly endorses CSA's approach and has committed the office's support. Private sector organizations interested in workable privacy solutions might find CSA's approach just what they are looking for.

Privacy At Work

Privacy in the workplace is an issue of rising concern, highlighted by the decision during the year of two major companies (Toronto-Dominion Bank and Exxon Canada) to introduce drug testing programs. Previous studies by the Office of the Privacy Commissioner have stressed the very limited utility of drug testing programs, and have concluded that the results to be gained do not justify the intrusive methods required. Developments in the past year suggest that the time has come to consider means by which individual privacy rights can be accommodated in areas of industrial activity which have special safety or other problems. It is not the Commissioner's view that no case can ever be made for testing programs; it is decidedly his view that such programs must meet demonstrated tests of both need and effectiveness.

Fine-tuning the Act

The *Privacy Act* has been part of the landscape for nine years, long enough for observers to form at least some interim judgments about its effectiveness. It is entitled to high marks.

The doctrine of fair information practices which is the heart of the *Privacy Act* has proved highly adaptable to a wide variety of situations in a rapidly-changing environment, and gives every sign of long life expectancy. Certainly, a better set of principles has yet to be devised.

The chief limitation of the Act is that it applies only to records in the custody of the Government of Canada and some of its agencies. Fair information practices have found their way into the laws of only a few other jurisdictions, and hardly at all into the private sector. So by far the largest part of personal information holdings in Canada continues to be unprotected.

Unless and until that situation changes, the *Privacy Act* will continue to be the most important piece of privacy legislation in the country, both for the immense holdings of personal information it covers in the Government of Canada, and for the benchmark against which data protection standards in other areas can be measured.

Thus, while the Act has weathered well, it needs to be constantly re-assessed, not in the sense of major overhaul but, if the phrase may be used, of "polishing the jewel". One comprehensive parliamentary review took place in 1986-87, as required by subsection 75(1) of the Act. But six years of added experience suggest it may be time for another.

Surprisingly though, we advise fine-tuning the Act's strengths: the definition of personal information (section 3), the fair information practices code (sections 4 to 8) and the access to personal records protocol (sections 12 to 28).

Redefining "personal information"

The *Privacy Act* architects could not have foreseen today's new technologies when they defined personal information. Advances in the science of genetics, for example, give added meaning to the words "information about an identifiable individual recorded in any form" (section 3—definition of personal information).

Locked in the smallest drop of body fluid or speck of tissue is a mountain of information that defines in minute detail the characteristics not only of individuals but also those of their forbears. Though paragraphs 3(b) and 3(d) refer to medical information and blood type, it is not clear that information recorded in biological samples about an identifiable individual falls within the scope of section 3. While it is clear the office would argue it does, any controversy regarding its inclusion could be eliminated by amending section 3. What is sought here is a clear statement that information contained in a genetic sample is personal information for purposes of the Act.

Some may argue that such an amendment is unnecessary tampering with an already elegant definition. But the genetic key is potentially so damaging to our privacy that a specific reference in the Act is needed.

Tightening up disclosures

Sections 7 and 8 of the Act are the foundation upon which are built our confidentiality rights. Its cornerstone is the principle of informed consent. Personal information cannot be used or disclosed without the concerned individual's knowledge and consent.

The *Privacy Act* demonstrates the truism that rules often need exceptions. Exceptions are necessary to strike a balance between an individual's right to confidentiality and the government's responsibility to manage the affairs of state. It is, for example, reasonable for personal information to be disclosed without consent to meet legal requirements or for criminal investigation purposes.

Curiously, one of the strengths of the legislation is contained in one such exception—paragraph 8(2)(m), disclosures in the public interest. The Act does not prevent public interest disclosures nor does it attempt to substitute detailed written rules for the reasoned and considered judgment of the head of an institution. It simply provides a transparent framework which ensures all interested parties are informed and that discretion regarding disclosure is properly exercised. The head of the institution who, after all, knows the records best, must balance the benefit to the public against the harm it may cause the individual.

However, most disclosures without consent do not require the head to exercise discretion. This may be delegated to staff. In this respect, the section is deficient. Staff should not be delegated the responsibility for consistent use disclosures; exchanges of information with foreign states or with the provinces; disclosures to investigative bodies, to Members of Parliament, to researchers, to auditors or to associations of aboriginal people. Since they are serious derogations from the prior consent principle, the head of the institutions should be required to decide on these disclosures.

This process might also resolve another difficulty with consistent use disclosures. Subsection 9(1) requires government agencies to notify the Privacy Commissioner of new consistent uses not recorded in *Info Source*—the personal information index. The office has received and assessed only 18 such notifications in its entire history. Our complaint and audit experience shows clearly that new consistent use disclosures are happening routinely without proper notification of the Commissioner. Surely higher level accountability would produce a more diligent application of all of the Act's requirements.

The Commissioner would welcome some fine-tuning of sections 7 and 8. The major flaw in the fair information practices code is its failure to provide a mechanism for an individual to prevent the release of personal information pending a determination of the propriety of its release. As previous annual reports have stated, it is an anomaly that individuals denied access to their personal information may go to court for review of the decision, but they cannot seek a review of a department's decision to disclose their personal information to third parties.

The *Access to Information Act* provides a mechanism for alerting third parties, such as corporations, whose sensitive commercial information may be shared. Yet, the *Privacy Act* provides no similar rights to individuals whose sensitive personal information may be disclosed. Does not personal information deserve protection from abuse that is at least the equal of that afforded corporate information?

True, in matters of national security or criminal investigations it may not be possible, or wise, to provide an individual with prior notice before disclosing sensitive personal information. These disclosures can be properly documented for the Privacy Commissioner's review.

Broadening the injury test

While the *Privacy Act* gives Canadians an impressive array of access rights, it also gives government institutions a vast—cynics might say limitless—arsenal of exempting provisions to defeat them. These exemptions are not unreasonable if they can be supported by clear, strong rationale. Most of them are. Who, for example, would want terrorists to learn that law enforcement agencies were hot on their trail, simply by applying for their records?

But some exemptions go too far. For example, government agencies can or must withhold personal information under sections 19, 22(1)(a) and 22(2) without demonstrating that release would cause some injury. These provisions concern, respectively, information obtained from other governments, law enforcement information, and information obtained by the RCMP while providing policing services to a province or municipality. Solicitor-client information (section 27) can also be withheld without a requirement to demonstrate that its disclosure would be harmful.

However, paragraph 22(1)(a) is certainly the most offensive. This section authorizes the government to deny access to personal information prepared "in the course of lawful investigations pertaining to the enforcement of any law of Canada or a province", provided the investigation was conducted by an "investigative body". There are nine such bodies listed in regulations to the *Privacy Act*. The exemption amounts to carte blanche to these bodies to deny Canadians access to their information for no reason whatever. No agency should be entitled to this kind of denial.

Generally this section has not been abused. The RCMP, for example, which has the right to use the exemption, rarely invokes it, preferring to use other sections of the Act. On the other hand, some cases demonstrate clearly how it can be misapplied.

One example concerned the Department of Consumer and Corporate Affairs (CCA). CCA's director of investigation and research investigated a complaint that the Parliamentary Press Gallery had violated federal competition rules when it denied an application for membership. CCA's investigation found no violation but, confronted with the complainant's subsequent privacy request for the opinions of Press Gallery members about his application, the department refused, taking refuge in paragraph 22(1)(a). Since CCA's investigation was complete, the Privacy Commissioner could find no valid basis for CCA denying the privacy request. However, the department was unyielding, and, given the blanket authority conferred by the section, he could do nothing more.

This kind of blanket exemption should be stricken from the Act. It has proved unnecessary even in such sensitive areas as police investigations. As it stands, it merely provides a convenient shield for bureaucrats not wanting to be troubled by the tiresome need to justify their decision. The following paragraph (22(1)(b)), with its injury test, provides a reasonable framework to allow government institutions to effectively manage their programs.

The scope of this exemption explains the Commissioner's reluctance to applaud additions to the list of investigative bodies. During the year, the Commissioner learned that three new bodies were being considered. The quarrel is not with the particular bodies being considered but rather with the concept of any investigative bodies at all. Other exemptions—subject to an injury test—provide all the latitude needed. The Commissioner's office is now part of a working group examining the exemption, its uses and some options for the future.

"Catch 22"

One final preoccupation about the Act needs addressing in this report.

Section 16 allows an institution to refuse to either confirm or deny the existence of personal information. To most of us at least, other exemptions provide a more than sufficient limitation to the general right of access. Section 16, though, goes far beyond the mere refusal to provide access.

The doctrine of refusing to confirm or deny is ingrained in Canadian security and policing psyches, and it would seem that section 16 is its statutory embodiment. As distasteful as the notion is in a free and democratic society, it may be necessary for us to tolerate its use in order to achieve a public good. But invoking this section with any exempting provision other than those concerned with security and policing (sections 21 and 22), would surely constitute an unacceptable encroachment on an already too highly encumbered and fragile right of access. The Act should be amended to limit this authority to national security and criminal investigations.

The threat to our privacy rights is compounded because though the Privacy Commissioner may investigate complaints about this section, he cannot reveal any information or even that there is no information!

Should the Privacy Commissioner be unable to resolve the complaint, he faces Catch 22. Simply by referring the matter to Federal Court he runs the risk of revealing the existence of information, thus breaching his own Act. The Act needs a mechanism to enable the Commissioner to refer these complaints to the Courts for adjudication.

Genetic Testing

It is easy to overlook the privacy implications of technologies many of us do not yet fully understand. Nowhere does this pose a greater danger than with genetic testing.

Advances in genetic technology promise to unravel medical mysteries, thus preventing many diseases and allowing treatment of others. The technology can already identify many genetic traits or disorders and, occasionally, accurately predict our genetic destinies. This news is good. But there is also the inevitable dark side. Genes can reveal deep secrets about individuals' physical and psychological being—secrets they may not want others to know, or may not want to know themselves. Stripping away the human being's very essence to the twisted strands of DNA molecules—the personal genetic building blocks — is an assault on privacy that few may want to endure.

Do governments or other organizations have a right to acquire personal genetic information “for the public good”, with or without consent? Or should individuals be able to protect their genes from inspection by either the state or the private sector?

This year the office completed its report, *Genetic Testing and Privacy*, the third in a trilogy on biomedical testing. (The first two dealt with HIV/AIDS and drug testing.) The latest report examines the issues flowing from the rapid development of genetic testing technology, including several present or potential uses. These tests could be designed to select genetically fit employees or monitor the effects of workplace hazards on their health; determine eligibility for such benefits or services as insurance; diagnose or predict medical conditions during regular medical care or reproduction (pre-conception, prenatal and neonatal), and provide more accurate forensic evidence in criminal investigations.

To date, genetic testing in Canada appears to have been limited to three fields — reproductive technology, regular medical care, and criminal investigations. Still, the advent of cheaper, more informative tests will almost certainly stimulate further interest in testing. Governments will not be the only intruders. Private sector interests, such as employers and insurers, will become increasingly enthusiastic about the supposed ability of genetic testing to give them a competitive edge.

Governments may be tempted to override serious ethical concerns and apply genetic knowledge to promote eugenics. Certainly today's world is not free from pressures to thus create "better societies". In the private sector, genetics could be used to identify genetically "inferior" individuals. For these unfortunate members of the genetic "underclass", access to employment or services could be severely impaired.

In both environments—government and private sector—people could find genetic traits over which they have no control determining how they will be permitted to lead their lives, with little concern shown for the person behind the genes.

This office was chilled by the potential growth in the number and types of intrusions that may ensue as genetic technology advances. Accordingly, the report recommends against mandatory (and, in some cases, voluntary) genetic testing in several situations. It also calls on the federal government to study the extent of genetic testing in Canada, and the likely future uses of this technology.

Prominent recommendations of the report are:

- every person should have a reasonable expectation of genetic privacy;
- governments should collect personal genetic information only if specific statutory authority permits;
- neither government nor the private sector should compel persons to learn their genetic traits or disorders;
- employers should not require genetic testing in employment, whether to identify undesirable genetic traits in employees or applicants, or to identify genetic changes due to workplace exposures; only true voluntary testing would be allowed;
- service or benefit providers should not be permitted to use mandatory genetic testing to determine a person's eligibility for services or benefits;
- governments should not collect personal genetic information relating to the reproductive process;
- governments should not collect personal genetic information relating to ordinary medical care;
- governments should restrict forensic DNA analysis in criminal investigations to identifying offenders or exonerating suspects;
- governments should not establish personally identifiable genetic databases or banks of genetic materials from the general population for crime control.

The report merely scratches the surface of genetic testing. The Commissioner hopes it will stimulate thought and action before powerful public or private sector interests transform us all from human beings into the mere sum of our genetic parts.

A Year in the Privacy Trenches

Telecommunications toys—playing with privacy

Readers of these reports may recall the former Privacy Commissioner's concern about the privacy threats in new telecommunications technology (1989-90 report, p. 26). The Commissioner cited Bell Canada's new Call Management Services (CMS)—and Caller ID in particular. The CRTC has since approved Bell Canada's service and similar ones are now available from most telephone companies.

Caller ID is just one element of the new telephone technology. Many new phone services are not features of improved telephone sets but the product of powerful computers which handle telephone switching operations. However, users do need specially equipped telephones to allow them to see and record the caller's phone number before picking up the handset.

Seeing the caller's number before answering may provide protection against harassing calls. But it also trades away the rights of others who have an equally legitimate desire to avoid having their phone number known or recorded.

This desire—or need—for anonymity is obvious for those calling crisis hot lines or for volunteers who often return calls from home. Many professionals—from psychiatrists to probation officers, from politicians to undercover police officers—may now be unable to call from home, not wanting their numbers displayed and recorded.

Many are also concerned about commercial use of their phone numbers. Anyone calling a business with a casual inquiry now courts the risk of having their number recorded, only to be called back for marketing purposes. Reverse directories (which list subscribers sequentially by phone number) can then link the number to a person and address.

Trading away everyone's privacy is a heavy cost for CMS' few benefits. Charging subscribers to **prevent** the display of their numbers means privacy is for sale and not everyone will be able to afford it.

These concerns are well-founded and workable solutions are elusive. CMS can vary from one phone company to another, making privacy protections a patchwork. Some companies allow callers to block the number display for all calls on their line—or just selected calls—but at a cost. Some charge nothing to block. Others offer a form of encryption which scrambles the number. Nearly all companies offer a solution for women's shelters.

One recent CMS decision comes from the Manitoba Public Utilities Board. The board approved Manitoba Telephone System's application for a trial run, providing that all subscribers benefitted from free call blocking. The board also demanded free line blocking for shelters and individual victims of abuse. However, the board did not approve Call Return—the option which traps the numbers of unanswered incoming calls and displays them later on command.

Of broader significance is the CRTC's recent announcement—well after the end of our reporting year—that phone companies under its jurisdiction must offer free per-call blocking.

Canada is not alone in its struggle to find appropriate solutions for technological advances. In the United States, the debate has raged since New Jersey introduced the service in 1987—a debate involving public utility commissions, state and federal legislatures and even the courts.

And the solutions range from New Jersey's, which offers no blocking at all, to Pennsylvania where CMS has been ruled illegal since it offends the state wiretap law.

Texas proposes that customers pay if they want to display and, most recently, an administrative law judge in California proposed that the state utilities commission prohibit Caller ID because it is not in the public interest and violates both the state and federal constitutional right to privacy.

Still other states offer free per-call blocking, pay-per-line, free per-call **and** per-line blocking. At the height of the debate, one company even offered a service to automatically refuse blocked calls. The options are dizzying.

The debate has focussed public attention on the privacy issue. Probably more disturbing is the knowledge that these services are only the beginning—an early feature of the ever-increasing intelligent network system. This system will soon offer personal communication networks with a lifetime personal phone number, dial-up services and picturephones. The technology is evolving so fast that neither engineers nor policy makers have time to consider the social impacts. Each new development affects or overrides the privacy protections so laboriously erected to defend against the last one.

Obviously the Privacy Commissioner's small office cannot keep abreast of each new technical marvel; it lacks the expertise and resources. Nevertheless, the Commissioner is eager to find enduring and workable solutions.

The New York State approach has substantial appeal. That state's public service commission took a broad policy approach to telecommunications privacy, approving eight privacy principles. They state, for example, that telecommunications companies should recognize clients' privacy explicitly and that customers should not pay extra to preserve their privacy status quo. Customers should be told of any proposed use of their information and be able to give informed consent to any further uses.

The office and the Department of Communications are both examining the broad issue of telecommunications impact on privacy and considering some remedies.

New Telecommunications Act

A step in the right direction may be the initiative in the proposed *Telecommunications Act* in which Parliament recognizes the privacy impact in telecommunications technology. The act includes as a policy objective

“...to respond to the economic and social requirements of users of telecommunications services, including the protection of the privacy of individuals. ...”

This act also allows the government and the CRTC to block such intrusions as unsolicited phone calls and junk faxes.

The office intends to monitor passage of this bill through the House to help ensure that the privacy protections are not eroded. At issue is whether its provisions go far enough. Either the act or its regulations should outline the privacy standards which telecommunications services must meet.

This year's SINs

Born without SIN

Resistance to demands for the Social Insurance Number (SIN) took an unusual turn this year when a Prince Edward Island couple refused to apply for a SIN for their newborn baby.

PEI's vital statistics department requires all newborns to be assigned a SIN for the province to use as identification numbers for its Health Service Payment Plan. The couple asked for an exemption and were denied. The health department responded by refusing all claims for the baby's medical care because she did not have a SIN.

The couple has taken the case to court, arguing that requiring the baby to have a SIN (and denying the medical claims) offends several provisions of the *Canadian Charter of Rights and Freedoms*. The parents maintain that their daughter has no legal obligation to obtain a SIN until she begins insurable employment. They argue further that denying the medical claims offends *Charter* protections against unreasonable search and seizure and denies the baby's right to equal benefit of the law, and requiring a baby to have a SIN breaches an individual's reasonable expectation of privacy.

The case is interesting to this office, although well outside the *Privacy Act*. But it does raise an important privacy question: what program or activity of Employment and Immigration Canada (the department responsible for issuing SINS) allows it to issue the numbers to newborns?

SINS were created for unemployment insurance and Canada Pension Plan, and later authorized for use by Revenue Canada for individual income tax reporting. Recent federal government policy—applauded by the Privacy Commissioner—has reined in many unrelated federal government uses of the numbers. However, apparently EIC still relies on a 1970 federal-provincial agreement concluded well before any federal privacy protection was in place.

The Commissioner has asked Employment and Immigration to identify a direct relationship between assigning SINS for birth registration and EIC programs. If none can be shown, he will urge EIC to reconsider its arrangement with PEI in light of both the *Privacy Act* and the federal government's policy to restrict SIN use to a short list of social programs.

Casting the first stone— renumbering the public service

One significant impact of the federal policy to restrict its own use of SIN is the need to re-number some 310,000 public servants, members of the military and RCMP.

Supply and Services Canada (which controls the pay and records data bases) will begin assigning new Personal Record Identifiers (PINs) by January 1993. Each employee will receive two numbers: the PIN and a second number to be given to third parties such as banks, insurance companies and the employees' unions. This second number will ensure that employees' PINs remain private but allow the employer to link third party transactions to the correct employee.

There remains some confusion about what constitutes a proper request for a person's SIN. For example, the Public Service Commission's language testing programs still ask employees to volunteer their SIN and public service unions continue to use SINs for membership purposes. These are legitimate requests. But once the renumbering is completed, the Commissioner urges federal employees to keep their new PIN to themselves.

SIN or else

The Commissioner's office was alerted to what seemed to be an unnecessary use of SIN in Employment and Immigration Canada's new automated Job Information Bank in St. John's, Newfoundland. The pilot project allowed job seekers to scan a computerized listing of available positions and select those that matched their interests and skills. The system gives applicants greater opportunity and frees up EIC staff for other duties.

However, a caller complained that he could not even look at the list without first providing his SIN. Since any casual passer-by can scan the paper notices of jobs available, he thought demanding a SIN for a computer listing was excessive and—since he was not claiming unemployment insurance—unnecessary.

Apparently EIC asked for the SIN to measure both the effectiveness of the system and its ability to place UI claimants. Responding to the office's enquiries, EIC acknowledged that the system should also accommodate non-UI claimants.

The system has now been modified. The opening screen advises users that access to the system is unrestricted. Those receiving unemployment insurance have the option of entering their SINs so that the Canada Employment Centre has a record of their job search. This change will become part of the new nationwide job-bank system.

Technology update

Last year the Commissioner reported on Employment and Immigration Canada's (EIC) plans to harness new information technology to handle the department's huge client load. EIC had pilot projects underway using smart cards and an automated telephone answering service (AVRES).

EIC is not the only federal department considering using new information technology to improve service. Veterans' Affairs has already tested smart cards as a method of improving its delivery and billing of prescription drugs to veterans. Revenue Canada is looking at the possibility of having travellers use the cards to declare goods or pay fees at customs points.

Several departments are jointly developing smart cards which would allow remote access to government computers. This would permit someone working at a home personal computer to communicate with a government agency's computer over the telephone.

As with much of the new communication technology, there are privacy implications.

The smart card is like a conventional bank or credit card—but with an essential difference. Smart cards are imbedded with an integrated circuit chip which gives the card intelligence for processing and memory for storing data. Chips and digitized information also make it possible for the cards to carry an invisible photograph or even a fingerprint of the bearer. The cards could be used to provide banking, telephone and medical services, giving the user access to a network of computers.

Privacy needs

Clearly smart cards are an important technical advance which can improve service to clients and control costs for departments—particularly those like EIC which must track, credit deductions for and pay benefits to such large numbers.

Yet government agencies and their clients should be able to enjoy the benefits of progress without sacrificing individuals' control over their personal information. In effect smart cards could become that universal identity card that North Americans so fiercely resist. Their development invites a profound shift in the relationship between the individual and the state.

This can be avoided, first, by making the systems transparent to the clients. Card bearers must know their inherent rights when using the card, what information the card contains, how it will be used, and what risks that use implies.

Individuals should be free to refuse the card without jeopardizing their access to the service. And similarly, holding a card should not confer advantages unavailable to those who opt out.

Finally, the systems and their participants must respect both privacy laws and basic ethical principles on collection, handling and disclosure of personal data.

Because of the Commissioner's concern about the security aspects of the pilot projects, his staff were invited to join two federal government working groups: one dealing with applications of the technology and the other developing standards for remote access to computer systems.

The applications group—whose ultimate goal is to establish standards and guidelines for all government smart card applications—will identify how government might use the cards and the framework in which they should operate. Its membership includes such federal agencies as Health and Welfare Canada, Supply and Services Canada, the RCMP and Veterans' Affairs, as well as the Quebec and Ontario health ministries.

The office is also a member of a special interest group working on the development of remote access to computer systems. Since many government agencies have a common interest in access, they are sharing research and development costs and contributing to shared standards.

The AVRES Project

Last year's report (p.53) described a privacy flaw in EIC's automated telephone inquiry system being tested in Quebec City. The story ended unsatisfactorily since the project seemed too far advanced to change. However, EIC has re-written the ending and the Commissioner could not be more pleased.

The system allowed claimants with touch-tone telephones to call into a computer for routine information about their own unemployment insurance claims. For example, a caller could confirm that his or her claim had been accepted and when benefits would begin. Callers identified themselves by their Social Insurance Number (SIN) and birthdate. The office heard about the service when a local radio station questioned this use of SIN.

There was no question that EIC could use SINs to identify UI claimants—the numbers were devised for this purpose. But the Commissioner was concerned about the lack of security of the SIN-birthdate combination. The office discussed the problem with EIC staff who agreed that both pieces of personal data are widely available and therefore not a secure access code. However, the test project had already expanded to London and Peterborough and it seemed too late for changes.

Nevertheless, aware of the Commissioner's concern, EIC systems designers used the Peterborough project to test a new four-digit telephone access code similar to a bank number.

Apparently the test was successful and the new code will be a feature of the national program. EIC will assign claimants the number to identify themselves when making telephone inquiries. Claimants may also choose their own numbers.

The Commissioner applauds EIC's quick response and its sensitivity to client security.

Data Matching

Probably the most important data matching news this year is what did not happen—apparently data matching did not happen. The Commissioner received just three notifications during the entire year—all from Agriculture Canada.

The Commissioner wishes not to appear suspicious. Yet it would be credulous to accept that of more than 150 federal agencies subject to the government's data matching policy, only one began any new matches of discrete sets of files during 1991-92.

The matching policy restricts linkages between computer data bases that could produce detailed dossiers—or "super files" on individuals. It also requires federal agencies to submit matching proposals to the Commissioner 60 days in advance. He then assesses the match against a set of criteria and acts as an advocate for the subjects of the files. The intent is to prevent government efficiency from trampling individuals' personal information rights.

The policy, while admirable, may not be working. Only 22 federal agencies describe anything remotely resembling a data match in their listings in *Info Source*—the federal information directory. Some departments couch matches under more benign headings like “use” or “disclosure”. And others only recognize a match when it links with data from an outside agency, contrary to the policy which also controls matches of different program files within an agency.

Everything the Commissioner has seen leads him to conclude that computer data matching is common in government—particularly with social programs, law enforcement and intelligence operations and the criminal justice system. Do government staff recognize a data match? Are they unaware of the policy? Or do they simply see the policy as a nuisance to be avoided?

The Commissioner urges the Treasury Board to investigate. In the meantime, the Commissioner’s compliance auditing teams have added data matches to their list of audit criteria.

Agriculture Matches

In fairness, Agriculture Canada has been scrupulous in observing the data matching policy. Its first notice advised that the new *Farm Income Protection Act* would allow Agriculture to match farmers’ information from the income stabilization account with income information from Revenue Canada.

The match will ensure that the benefits farmers receive from these programs are based on correct information about their revenue, expenses and production. The act gives Agriculture legal authority for the match and allows it to use the Social Insurance Number.

Garnishees for Family Support: Agriculture also advised the Commissioner that it would match information from the Western Grain Stabilization Program with the Department of Justice to allow garnishee of program payments from farmers who had defaulted on their family support. In fact, the submission was unnecessary because Parliament had passed a regulation under the *Family Orders Agreements Enforcement Assistance Act* authorizing deductions from the stabilization program.

More Information Needed: Finally, the Office was notified of a match between Farm Debt Review Board files and Quebec agriculture department records. The match supports a new program to subsidize beef feed lot operators and to mediate with farmers' creditors. The Office has not received sufficient detail to assess this match.

Complaints Directorate

The office received 1,402 new complaints this year compared with 1,239 last year—an increase of 13 per cent. This increase is consistent with the pattern established since the office opened in 1983. Not consistent is the drop in the number of completed cases—782 cases were closed, 269 of which were well-founded, 448 not well-founded and 65 discontinued.

The 1991 Census

During the past year, one issue has consumed considerable time—investigating 34 complaints against the 1991 census. Several complainants were concerned about Statistics Canada's collection of personal information and had refused to respond to census questions they considered an unacceptable invasion of their privacy.

Others cited the guarantee (or lack) of confidentiality of their census responses. The most frequent complaint was that census workers who gathered the results were neighbours or acquaintances of the complainants. Complainants believed that their completed questionnaires would be sent directly to Statistics Canada in Ottawa to be reviewed by some anonymous bureaucrat, not by someone from their neighbourhood. The investigation is now in its final stages and its results will soon be shared with Statistics Canada.

This is the first time this office has undertaken such a complicated and time-consuming investigation, and it has taken its toll. The nearly six months spent by three senior privacy officers who spearheaded the investigation took time away from other cases. This is the main reason that the number of completed cases is lower than last year. Staff turnover (and subsequent training) has also contributed, thus exacerbating a growing backlog.

A New CPIC Policy

The Canadian Police Information Centre (CPIC) continues to be the target of complaints and inquiries about the collection, use and disclosure of personal information held in its databases. CPIC is a collection of police databases, federally funded and administered by the RCMP. However, it is governed by an advisory committee of major municipal and provincial police forces who contribute and have access to the information.

We often hear from individuals who cannot get access to their own information in CPIC because various police forces cannot disclose information contributed by others. For example, CPIC may not disclose personal information contributed to it by the Ottawa City Police.

This office has discussed its concerns about CPIC's administration in earlier reports and recommended that the RCMP consult other CPIC users about introducing voluntary privacy controls over its databases. This would provide comprehensive protection for CPIC's collection, use and disclosure of personal information, and allow individuals to access and correct their personal data.

Congratulations are in order. CPIC approved and implemented a CPIC Code of Ethics in November 1991, one which generally addresses the Commissioner's concerns—particularly those dealing with access rights. It entitles individuals to request access to their personal information maintained on CPIC and to correct it, when necessary.

Top Ten

Last year, for the first time the office listed its top ten clients—a group which accounted for 80 per cent of the total caseload. Eight of those ten departments made the list again this year: Correctional Service Canada (CSC), Canada Post Corporation, Employment and Immigration Canada, Revenue Canada-Taxation, National Defence, Canadian Security Intelligence Service(CSIS), RCMP and National Archives.

Joining the top ten is the Immigration and Refugee Board (IRB) with 68 complaints received—the first privacy complaints received against IRB. However, 67 of those were made by one person, including 33 time limit complaints which were considered well-founded. Investigation of the 33 access complaints continues.

Completed Complaints by Grounds and Results

		Disposition				
Grounds		Well-founded	Well-founded: Resolved	Not Well-founded	Discontinued	TOTAL
Access		5	102	260	41	408
	Access	5	100	228	41	374
	Correction/Notation	0	0	29	0	29
	Index	0	0	3	0	3
	Language	0	2	0	0	2
Privacy		5	12	92	13	122
	Collection	1	2	35	4	42
	Retention & Disposal	1	1	6	6	14
	Use & Disclosure	3	9	51	3	66
Time Limits		142	3	96	11	252
	Time Limits	138	3	90	11	242
	Extension Notice	4	0	6	0	10
TOTAL		152	117	448	65	782

Another significant increase occurred at Revenue Canada-Customs and Excise. Their 72 complaints constitute a five-fold increase over last year's figures.

Last year's report applauded CSC for its efforts to conquer its delay problem. Unfortunately CSC's delay complaints more than tripled this year—160 (compared with 50 last year). These delays account for 34 per cent of the year's time limit complaints. However, this warrants an explanation. CSC has changed the way it processes information about inmates that it receives from provincial and municipal governments and police forces. CSC routinely used to exempt information received in confidence from another government. However, after years of urging from this office, CSC now asks the originator whether it will agree to disclose.

This causes delays for applicants. With heavy caseload and shrinking resources, CSC has to choose between two evils: providing a less than complete response in time—or go the extra mile, risk exceeding the time limits but provide the applicant more information.

Other departments also continue struggling to meet time limits: National Archives, Revenue Canada-Taxation and National Defence.

Toward the end of the reporting year, the office changed the way it reported time limits complaints. Frequently, complainants question departments' claims of a time extension either to consult other organizations or because operational requirements prevent them from responding within 30 days. The office did not count the number of complaints specifically questioning the notice. But time limits complaints have now been divided into two categories: time limits and extension notices. The change acknowledges the distinction between the two issues. It also identifies departments which continue to neglect their responsibilities to respond in time.

At a time of government restraint it is difficult to chastise departments for not respecting the time limits. Budgets and staff have been slashed in most government departments with the result that service to the public suffers.

While the number of time limits and access complaints received increased by 31 per cent from 855 last year to 1118 in 91-92—the number of complaints about improper collection, use and disclosure dropped by 26 per cent—from 384 in 90-91 to 284 in 91-92.

How Institutions Measured Up

The RCMP continues to carry the banner for maintaining its high regard for the letter and spirit of the Act. Only one of its complaints was well-founded, resolved; 40 were not well-founded, while three were discontinued. CSIS too must be commended; of the 56 complaints completed last year, only five were considered well-founded, and all were resolved.

Last year CSC had the highest ratio of well-founded complaints, with EIC, Taxation and DND not far behind. This year, despite continuing to head the list of complaints received (a total of 287), only 27 per cent of all CSC's complaints were well-founded. Approximately one-half of the complaints against EIC and Taxation, and 32 per cent against DND were well-founded.

This year's number of discontinued findings is high—65 represents eight per cent of completed cases. However, the majority were discontinued when the office's initial notice to the departments prompted them to resolve the problem. Of course, that's what the ombudsman's role is all about—resolving problems, not counting complaints.

Top Ten Departments by Complaints Received

		Grounds		
Department	TOTAL	Access	Time Limits	Other
Correctional Service Canada	287	92	160	35
Canada Post Corporation	143	101	3	39
Employment and Immigration Canada	135	72	26	37
Revenue Canada, Taxation	107	27	59	21
National Defence	99	20	63	16
Canadian Security Intelligence Service	87	77	10	0
Royal Canadian Mounted Police	84	67	4	13
Revenue Canada, Customs & Excise	72	29	31	12
Immigration and Refugee Board	68	33	33	2
National Archives of Canada	47	14	23	10
OTHER	273	119	55	99
TOTAL	1,402	651	467	284

Proposals for New Exempt Banks

The office was consulted twice during the year on proposals to create new exempt banks. The RCMP advised the Commissioner that it intended to seek Cabinet approval to create an exempt bank for its National Security Investigation Records. CSIS also notified the Commissioner of its proposal to seek an exempt bank for its Investigation Records.

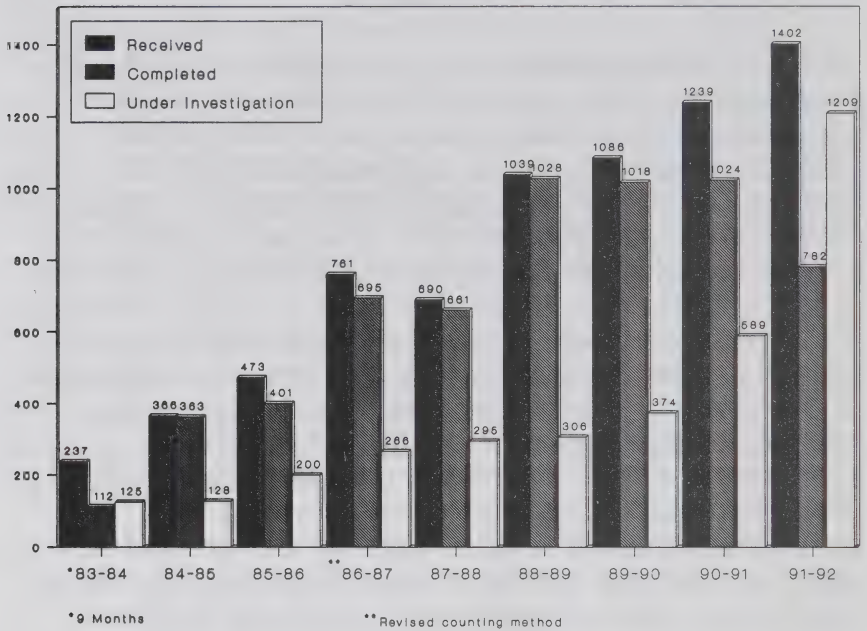
A staff review of both banks determined that they consist predominantly of personal information obtained or prepared during criminal investigations or whose release could damage the conduct of Canada's international affairs or defence (sections 21 and 22 of the *Privacy Act*). The Commissioner would not comment personally on the validity of the exemptions in order to avoid any conflict of interest should he receive a complaint about information contained in the files.

The Constant Plea for More Resources

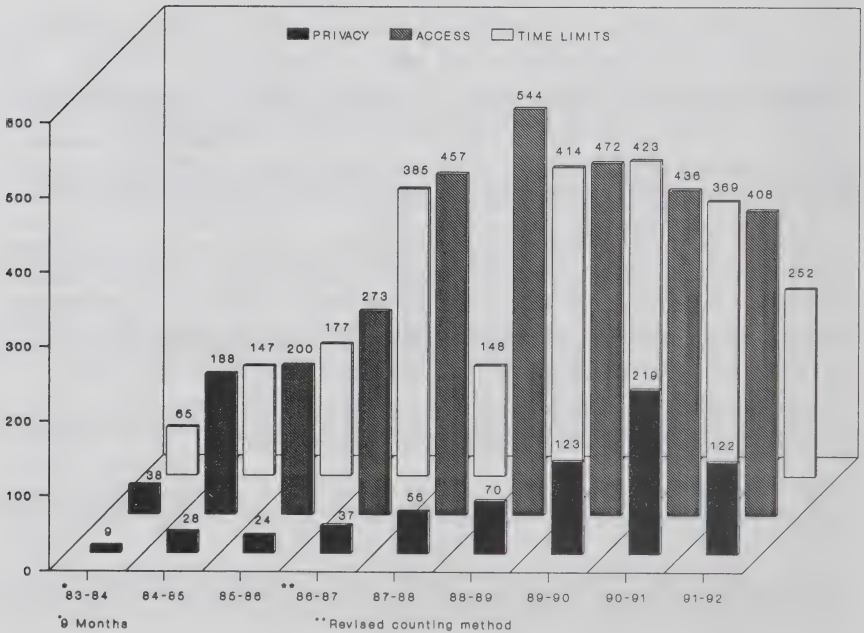
The 13 per cent increase in new complaints has put the office behind by almost a full year's caseload—1209 cases pending at year end. As predicted in last year's annual report, the backlog increased investigators' workloads to 200 each. Thus clients are now kept waiting sometimes months longer than they should to receive the Commissioner's finding.

Treasury Board allotted the office two additional person years to hire more privacy officers. But if new complaints continue to arrive at last year's pace, the office faces the spectre of more than 2000 open cases. This risks becoming unmanageable.

Completed Complaints 1983-92

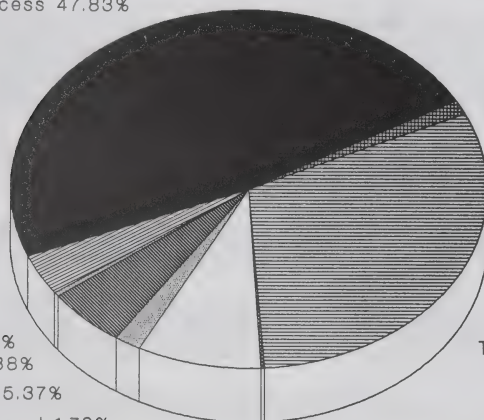


Completed Complaints and Grounds 1983-92



Complaints Completed by Grounds 1991-91

Access 47.83%



Extension Notice 1.28%

Time Limits 30.95%

Retention & Disposal 1.79%

Use & Disclosure 8.44%

Language 0.26%

Correction/Notation 3.71%

Index 0.38%

Collection 5.37%

Origin of Completed Complaints

Newfoundland	5
Prince Edward Island	4
Nova Scotia	43
New Brunswick	20
Quebec	48
National Capital Region Quebec	17
National Capital Region Ontario	114
Ontario	226
Manitoba	28
Saskatchewan	30
Alberta	94
British Columbia	144
Northwest Territories	4
Yukon	2
Outside Canada	3
TOTAL	782

Completed Complaints by Department and Result

Department	Dispositions				
	Total	Well-founded	Well-founded; Resolved	Not Well- founded	Discontinued
Agriculture Canada	3	0	2	1	0
Atomic Energy Control Board	1	0	1	0	0
Bank of Canada	2	0	1	1	0
Canada Post Corporation	67	2	9	55	1
Canadian Human Rights Commission	2	0	0	2	0
Canadian Radio-Television and Telecommunications Commission	1	0	0	1	0
Canadian Security Intelligence Service	56	0	5	42	9
Commissioner of Official Languages	1	0	1	0	0
Communications	1	0	0	1	0
Consumer and Corporate Affairs Canada	9	0	0	3	6
Correctional Service Canada	130	10	25	76	19
Employment and Immigration Canada	71	11	22	30	8
External Affairs Canada	13	0	7	6	0
Farm Credit Corporation Canada	1	0	1	0	0
Fisheries and Oceans	10	1	1	8	0
Forestry Canada	1	0	0	1	0
Health and Welfare Canada	7	2	0	5	0
Immigration and Refugee Board	34	33	0	0	1
Indian and Northern Affairs Canada	11	7	0	4	0
Justice Canada	8	0	1	7	0
Labour Canada	3	2	0	1	0

Completed Complaints by Department and Result

Department	Dispositions				
	Total	Well-founded	Well-founded; Resolved	Not Well- founded	Discontinued
National Archives of Canada	10	2	1	6	1
National Capital Commission	1	0	0	1	0
National Defence	110	25	10	65	10
National Parole Board	35	6	5	23	1
Office of the Superintendent of Financial Institutions Canada	3	2	1	0	0
Privy Council Office	1	0	0	1	0
Public Service Commission of Canada	6	0	3	2	1
Public Service Staff Relations Board	1	0	0	1	0
Public Works Canada	2	0	0	2	0
Revenue Canada, Customs and Excise	25	15	4	5	1
Revenue Canada, Taxation	67	31	4	31	1
Royal Canadian Mint	1	0	0	1	0
Royal Canadian Mounted Police	44	0	1	40	3
Secretary of State of Canada	2	0	0	1	1
Solicitor General Canada	5	0	0	5	0
Statistics Canada	3	0	0	1	2
Supply and Services Canada	7	1	0	6	0
Transport Canada	20	2	12	6	0
Veterans Affairs Canada	7	0	0	7	0
TOTAL	782	152	117	448	65

Some Cases

CPIC limits AIDS identifiers

A group of community organizations in Vancouver asked the Privacy Commissioner to look into allegations that Canadian Police Information Centre (CPIC) databases identified individuals as HIV positive.

Although no one could point the finger at a specific incident—and the office's jurisdiction over CPIC is questionable—the Commissioner decided to inquire informally.

The RCMP (which administers CPIC) explained that individual CPIC files could contain a “C” flag to indicate that the person has a contagious disease. The flag helps police find individuals with communicable diseases who have escaped from penitentiaries or wandered away from hospitals. It also helps police inform those who may have been exposed to disease.

The CPIC advisory committee asked for a legal opinion on identifying HIV/AIDS carriers. As a result, CPIC policy now forbids identification of carriers unless they have threatened to transmit the condition using physical violence or, for example, if a carrier has violated the public health act by willfully spreading the virus.

CPIC contacted all CPIC users to explain the new policy and a subsequent audit identified 96 “C” entries (not necessarily HIV/AIDS). Since then CPIC has reminded users and done yet another audit which found fewer than 40 “C” files remaining—all for *bona fide* law enforcement reasons.

Finally, an RCMP member and the privacy investigator met the coalition members in Vancouver to brief them and answer questions. The coalition appeared satisfied with the outcome. The Commissioner is particularly grateful that CPIC and the RCMP were willing to listen and respond to the group's real concerns.

Respondent should see entire file

A complaint about the Public Service Commission's handling of an application to see a personal harassment investigation file revealed what seemed to be inconsistent treatment.

The applicant (the respondent in the harassment case) was given only those parts of the file that PSC considered his personal information. The investigation revealed that PSC processes harassment files differently, depending on who is the applicant. When the applicant is also the complainant, PSC considers the entire file that individual's personal information and discloses everything except that which may be exempted under the *Privacy Act*.

However, when the applicant is someone else—for example, witnesses or the respondent—PSC processes only those records considered to be the applicant's personal information.

The privacy investigator considered that since the applicant was also the alleged harasser and lone respondent—and the entire file dealt with the investigation of a complaint against him—PSC should process the entire file.

PSC officials have agreed that when the respondent is an individual (rather than the department), it will process privacy applications from both complainants and respondents in the same way. This means that all information on the PSC investigation file will be disclosed unless it may be exempted under other provisions.

Since the applicant had not been denied access to any of his own personal information, his complaint was not well-founded. However, his complaint prompted PSC to disclose the remainder of the file which did not qualify for exemption and to change its processing methodology.

New spouses get equal treatment

An employee of the Communications Security Establishment (CSE) told his supervisors of his pending marriage, a requirement of all federal employees holding a secret or top secret security clearance. The employee provided his bride's name, birthdate, address and name of present employer—as required by the government's Personnel Security Clearance Questionnaire.

However, CSE also requested details of the new spouse's residence and employment from the previous five years. At that point, the woman complained to the Privacy Commissioner that CSE's demands for more information invaded her privacy. She also held that CSE should have asked her directly for the information and not collect it from a third party.

The investigation revealed that CSE's policy on security reliability checks was inconsistent with most other federal government departments which rely on the information on the employee's security questionnaire. As well, new CSE employees are not required to provide the more detailed information about spouses. Only established employees who change their marital status must provide their new mate's residence and employment history.

DND was the only other department found to demand this supplementary information in similar circumstances, asking for details of residence and employment over the previous ten years.

Without question, details of relatives' personal history is needed to conduct background checks on those in a position to influence employees with access to national security secrets. However, it was difficult to understand why CSE needed more personal history of new mates of its established employees than of spouses of new employees.

CSE officials were persuaded to bring their policy in line with other departments. Ironically, before the Commissioner's office pursued the matter with DND, its policy had already been amended.

The complaint was well-founded but resolved.

Bulletin boards no place for grievance responses

A National Defence employee complained to the Commissioner that his supervisor had posted on a bulletin board DND's response to his formal grievance about smoking in the workplace. The department's letter included his name, address and comments on DND's policing of its anti-smoking policy.

The investigation found that indeed the letter had been posted in the room where the complainant worked, in full view of other civilian and military employees. Apparently a manager had told the man's supervisor to post the letter as a reminder to personnel to comply with the anti-smoking policy.

Following the investigation, DND agreed that the personal letter should never have been the mechanism for reminding employees not to smoke in DND buildings. DND has ensured this will not happen again.

The Commissioner considered the complaint well-founded.

Employees' personal papers not for disclosure

During its investigation of a harassment complaint Revenue Canada-Customs searched the office of an employee it suspected of writing an anonymous note found on a colleague's desk. Revenue Canada investigators photocopied the employee's personal phone directory and took documents from his personal files to have analyzed by handwriting experts.

Discovering this, the employee complained to the Privacy Commissioner that Revenue Canada had improperly disclosed his personal information. The Commissioner's investigation established that personal documents had been taken; used during the harassment investigation, and disclosed outside the department without the complainant's consent.

The documents included employee benefit statements—including some medical information—and his completed personal record form which lists education, previous employment, personal references and identifies family members, their occupations and addresses. The Commissioner concluded that the use of this type of personal documentation during an internal investigation could hardly be “consistent” with the original collection purpose. He considered the complaint well-founded.

Revenue Canada-Customs has apologized to the complainant for disclosing the documents and has amended its investigation manual to prevent investigators from using such personal information without the individual's consent.

Anonymous tipster not EIC

A complainant alleged that Employment and Immigration Canada (EIC) had disclosed to his ex-wife information about his earnings from his unemployment insurance file. She then used this information in a court application to increase his support payments.

The investigator interviewed the two EIC employees who dealt with the complainant, both of whom denied disclosing any of his personal information to any unauthorized persons. The ex-wife and her current husband were also interviewed. They too denied having obtained the information from EIC, saying that the tip-off came from an anonymous caller.

The Commissioner concluded that there was no evidence to support the man's allegation that EIC staff were the source of the information and he dismissed the complaint.

Complainant revealed identity himself

A man complained to the Commissioner that Employment and Immigration Canada (EIC) officials had identified him to an EIC-funded organization as the applicant seeking information about it under the *Access to Information Act*. The complainant correctly observed that identifying him as the applicant was an improper disclosure of personal information.

The investigation established that the complainant had had a dispute with the managers of the organization which provides on-the-job training to otherwise unemployable individuals. The complainant then made annual access requests to EIC for information about the organization. He was well known to its staff and is alleged to have spoken openly about his requests for the centre's records.

When the latest request arrived, the manager simply assumed it was from the same person. As he said: "it didn't take a rocket-scientist to figure it out".

Without evidence to support the allegation that EIC revealed the source, the Commissioner concluded that the complaint was not well-founded.

Can mail blind persons' audio tapes "sealed"

A blind person complained that Canada Post's requirement that letter and talking book tapes be mailed unsealed violated his privacy rights.

The investigator found that blind persons can mail audio tapes free of charge. However, the material must be packaged so that Canada Post personnel can open it easily to ensure that it meets the regulations.

The complainant agreed to have the investigator discuss the matter with the Canadian National Institute for the Blind (CNIB). CNIB explained during the meeting that its free postage privilege amounts to an almost \$3 million a year subsidy, which CNIB is reluctant to jeopardize.

Cassette tapes must be sent in special padded mailers. For talking books (the bulk of its mailings) CNIB has developed a re-usable plastic pouch with a Velcro closure. According to CNIB, this is as much for convenience as for ease of inspection. For other mailings, small padded envelopes are used and are either taped or stapled shut. Canada Post does not object to taping or stapling and the CNIB had never heard of a blind person being challenged on this type of closure.

CNIB pointed out that the regulations require that the closure permit easy inspection of the contents. It does not forbid sealing the envelopes. He suggested that the complainant simply staple his envelopes shut so that it would be relatively easy to tell if the envelope had been opened.

CNIB illustrated Canada Post's flexibility on the use of the free mailing privilege with anecdotes of blind individuals mailing back their cassette players to CNIB for repairs, claiming (and receiving) the free mailing privilege. According to CNIB, these mailings are definitely not covered by this privilege.

The investigator explained the entire procedure, as well as the CNIB's position, to the complainant. He was satisfied that Canada Post was not unnecessarily violating his privacy rights. The Commissioner concluded that the complaint was not well-founded.

Disclosure an error—but whose?

A complaint against the RCMP illustrated that sometimes it is impossible to get to the root a problem.

A man complained to the Commissioner when he learned that the RCMP had sent an unsolicited copy of his fingerprints and criminal records to Canada Post. There was no apparent reason for this disclosure since the man had received a pardon for his conviction. The records should have been sealed.

The investigator was unable to get a satisfactory explanation—audit trails were unclear and eventually the Privacy Commissioner's decision had to be based on "best available" information.

The investigation showed that in early 1991, Canada Post security received a copy of the complainant's criminal history record from the RCMP. Although this is normal procedure when its employees or candidates undergo security screening, security staff had no record of requesting the information. The complainant was not a employee, nor was he an applicant for a position. The record was put in a "pending" file.

At the investigator's request, the RCMP examined its records and found the distribution notation "Post Office, Ottawa" next to the man's criminal conviction listing. However, this did not explain why it had sent an apparently unsolicited copy of the record to Canada Post.

Further inquiries showed that the man had been briefly employed by Canada Post more than 10 years before. A reliability check (including fingerprinting) was done at that time. This explained the original distribution reference to the post office. Once he left the position, his personnel records—including his fingerprints—would normally have been transferred to the National Personnel Records Centre.

The complainant, once again a federal government employee, recently underwent a periodic review of his security clearance. This required the RCMP to process his criminal history record. Since no-one had removed the distribution notation on the old record, the updated record was sent to Canada Post.

This explanation is largely a reconstruction of events based on probabilities; it is not definitive. The Privacy Commissioner concluded that there had been an improper distribution of the information but, given the lack of detail, he could not say who was responsible.

However, he was able to reassure the man that Canada Post no longer possessed either the fingerprints or criminal history record and that the information had been well-protected for the brief period it was in Canada Post hands. The RCMP no longer has the fingerprints.

Denial “legal” but unnecessary

An Ottawa man asked the Commissioner to investigate his complaints against Consumer and Corporate Affairs (CCA), including one that alleged it had improperly denied him access to his personal information. He had lodged a complaint with CCA under the *Competition Act* and, unhappy with the investigation, wanted to see the comments about him in the file.

The Commissioner's investigation confirmed that CCA had withheld some information collected by its Director of Investigation and Research (DIR), claiming that it had been collected during a lawful investigation. Since the directorate is one of those units identified as "investigative bodies" in the *Privacy Act*, paragraph 22(1)(a) allows it to refuse to disclose information obtained in the course of its investigations.

The information requested was collected while DIR was investigating a complaint under the *Competition Act*. Thus it was lawful to refuse disclosure. However, the Commissioner observed that the exempted information was relatively innocuous and the complainant probably already knew its substance. Yet, representations and reasoning failed to persuade CCA to disclose the information. It clung steadfastly to its right to refuse, despite there being no reasonable probability that giving the man the information would harm the investigation or any person.

Since section 22(1)(a) does not require CCA to satisfy an injury test, the Privacy Commissioner had to tell the complainant that—much as he disagreed with CCA's stand—it complied with the letter of the law. He had to find the complaint not well-founded.

Ontario Workers' Compensation files no longer "confidential"

A lawyer complained that Health and Welfare Canada denied him access to 20 pages from his client's Canada Pension Plan disability medical file which had originated with the Ontario Workers' Compensation Board (WCB).

At Health and Welfare's suggestion, the lawyer applied directly to the WCB and received more material than Health and Welfare had exempted, leaving him unable to determine which documents Health and Welfare had used to deny his client's application. He argued that he could not properly represent his client in a pension appeal without knowing exactly which documents the department had received from the WCB.

The investigator found that Health and Welfare had withheld 20 pages using section 19(1)(c) of the *Privacy Act*. This section requires federal institutions to exempt information supplied "in confidence" by provincial governments or their institutions. There is no flexibility or discretion.

Thus, once a provincial or municipal government claims confidentiality, federal agencies may not disclose the information regardless of how innocuous it may be.

The investigation confirmed that a December 14, 1983, agreement provided that all information from the Ontario Workers' Compensation Board to Health and Welfare Canada was confidential and not to be disclosed except by the WCB itself.

Despite the agreement, the investigator persuaded Health and Welfare to ask WCB officials for permission to release the material. Health and Welfare did so and, as a result, WCB changed its policy, authorizing Health and Welfare to release its information directly to applicants. Health and Welfare then disclosed the client's material to the lawyer.

This is an important policy change which should simplify the procedure for many applicants.

The Commissioner concluded that the complaint was not well-founded because Health and Welfare previously had no authority to release the WCB's records. He applauded the change of position.

Notifying the Commissioner

Forty-three times this year the office was notified by government agencies that they intended to release personal information "in the public interest" or to "benefit" an individual. The Commissioner's role in this process is simply to notify the person if he considers it appropriate. He may advise against—but not prevent—the release.

Staff examine these notices so that the Commissioner remains free to consider any complaints without having prejudged the disclosure.

Although section 8(2)(m) of the Act is intended for exceptional disclosures, many notifications have become repetitive and something of an administrative burden for both the department and the Commissioner's office.

For example, Multiculturalism and Citizenship routinely notifies the Commissioner when confirming the Canadian citizenship of nominees for the Order of Canada. Since this was a recurrent and routine use of citizenship documents, the office suggested the department acknowledge this publicly and change its listing in *Info Source* to describe this use of citizenship documents. The department agreed, eliminating paperwork for itself and providing the public a clearer picture of how citizenship information may be used.

Correctional Services disclosures—a reprise

Last year the Commissioner reported on the difficult balance between individuals' privacy and the public interest—particularly on the release of reports on two prison escapes during which three persons were murdered (see Annual Report 1990-91).

The solicitor general refused to give the Justice and Solicitor General Committee uncensored versions of the investigation reports, maintaining that the *Privacy Act* prohibited the disclosure.

His refusal became the subject of a question of privilege in the House of Commons and the then-acting Privacy Commissioner was called to testify before the Privileges and Elections Committee. The acting Commissioner saw no difficulty with the solicitor general providing uncensored reports to an *in camera* committee hearing.

The privileges committee report concluded "that there is nothing in the *Privacy Act* to prevent the House of Commons from issuing an order for the production of unexpurgated versions of the two reports. Accordingly, we do not believe that an amendment to the *Privacy Act* to permit such production is either necessary or desirable".

The report suggested making copies available to the Justice committee at an *in camera* meeting.

The following are samples of other public interest notices received during the year.

Release prompts complaint to Commissioner

The Privy Council Office (PCO) advised the office that it intended to disclose personal information about several individuals to a professional body inquiring into the conduct of two of its members. The documents had been produced in evidence before a federal commission of inquiry.

PCO had obtained the consent of one individual (who was not under investigation) but considered it impractical to obtain everyone's consent. The Commissioner's office believed that the individuals should be notified of the impending release but suggested that it would be less disturbing coming directly from PCO. Privy Council agreed and wrote to each person, setting out the reasons for disclosure and citing the permissive section in the *Privacy Act*.

One of the professionals under investigation objected and has since complained to the Privacy Commissioner.

Details released for possible bravery award

The RCMP advised the Commissioner's office that the Chancellery of Canadian Orders and Decorations (in the Governor-General's Office) had asked the Force for information on one victim of a 1972 Arctic plane crash. The Chancellery was considering awarding a posthumous bravery decoration to a young Inuit man who survived the crash and kept the injured pilot alive but died before both could be rescued.

The Chancellery was reconsidering the award following publication of a second book on the accident which detailed the young man's role in the pilot's survival.

The privacy investigator examined the material that the RCMP proposed to release and found it contained less personal detail than the transcripts of a coroner's inquest or either book on the crash. The proposed disclosure did verify the accuracy of some of the details in the book.

The office did not object to the release and concluded it need not notify the sole survivor since the information was already public.

Pilots and engineers list not released

National Defence (DND) asked Transport Canada for a list of helicopter pilots and maintenance engineers in the Ottawa area to notify them of job opportunities at DND.

The Commissioner's office is reluctant to support this type of wide-scale list disclosure when there are other means of communicating with the individuals. Disclosure might "benefit" those who got jobs, but not the other several hundred who did not. The office suggested Transport Canada mail notices for DND, or that DND simply place advertisements in local newspapers and professional journals.

Transport Canada decided not to provide the list.

Post-mortem to family doctor

A doctor asked National Defence for the post-mortem of a military member who died suddenly while jogging. The doctor was treating a member of the man's family and wanted to determine whether the officer had the same condition which could contribute to a heart attack. Since the condition is suspected of being hereditary, the doctor wanted to begin immediate treatment of other family members.

DND released the post-mortem, then notified the Commissioner's Office. Although the Office prefers to be notified in advance, the request arrived during the public service strike when DND had no office staff. There was no objection to the disclosure.

Korean veterans' list to Rideau Hall

The Governor General's Office was the source of another request for personal information, this time about Korean War veterans. This notice provided a good example of how easily communications can become muddled over the telephone.

The Chancellery asked Veterans Affairs Canada for access to its computer database containing personal information about veterans eligible for the Canadian Volunteer Service Medal for Korea. The personal details—names and addresses, language, service number and confirmation of eligibility—would speed processing of applications for the new Korean War medal. The Governor General's office wanted to present the awards in November 1991.

Veterans Affairs staff telephoned the Commissioner's office to discuss the request and were left with the impression that they would need written consent from each veteran. (In fact, consent was just one of the avenues suggested.) This message was conveyed to Chancellery staff who, understandably frustrated, called the offices directly.

Privacy staff asked to see a written notification and sample of the information to be taken from the database. Once they had examined material, it was apparent that everyone on the list had indicated an interest in the medal and therefore would benefit. Staff also suggested Veterans Affairs obtain a written undertaking that the Chancellery would use the data only for this purpose, then destroy it or return it to Veterans Affairs.

The misunderstanding was cleared up quickly and the Governor General presented the first of the medals at a ceremony in Ottawa on November 10, 1991.

False claim to Canadian citizenship

External Affairs advised the Commissioner's Office that it proposed to tell a foreign government that a man arrested overseas on drug-related charges was not a Canadian citizen, even though he carried a Canadian passport.

The foreign government had seized the passport and given it to External Affairs on the understanding that if indeed he were Canadian, Canada would issue travel documents once the man was released. Since he was not a citizen, the Canadian embassy would not provide consular services or travel documents.

The Commissioner's Office agreed to the disclosure because there is a significant public interest in the integrity of Canadian passports. And it is important that Canadians not be alarmed by reports of consular services being denied to "citizens" whose claims are actually false.

Inquiries—the Public Talks Back

Inquiries officers continue to respond to an ever-mounting tide of letters and telephone calls—4,671 of them during the year. The offices' national toll-free line (shared with the Information Commissioner) is the only nation-wide access and privacy information service.

Canadians are becoming more aware of existing privacy protection, as well as new or proposed legislation governing provincial and municipal governments. Saskatchewan has just proclaimed its *Freedom of Information and Privacy Act*, and both British Columbia and Alberta have promised similar legislation in their latest throne speeches.

However, callers are shocked to discover that the private sector remains totally unregulated. The office handles many calls from individuals faced with difficulties in examining or protecting their information held by private organizations. It is frustrating to confess that there is nothing the office can do since our jurisdiction is limited to the federal government. Even worse is being unable to suggest a route to solve many callers' problems.

Although the *Privacy Act* is a federal law, hundreds of federally-regulated agencies and companies, and most Crown corporations, are "unregulated"—including Canadian National Railways, Via Rail, Air Canada, Atomic Energy of Canada Limited, various ports corporations, telephone companies and financial institutions such as banks and insurance companies.

The office has also answered calls about handling personal information in MPs' offices and at the Royal Commission on the New Reproductive Technologies. Employees and clients are dismayed to hear that we cannot intervene nor can they use provincial or municipal laws.

A substantial part of the inquiries officers' time is spent explaining the limited controls on use of Social Insurance Numbers (SIN). Most believe SIN use was restricted by the legislation which created unemployment and pension programs in the 1960s. Despite promises made at the time, that is not so. Many callers find it difficult to accept that only the federal government limits its use of SINS.

Individuals too often must choose between protecting their SIN or getting the goods and services they want. Given our limited mandate, staff now encourage callers to write to their MPs in the hope that if more MPs hear the complaints, they might act to control unnecessary uses of the SIN.

But the SIN story is not all gloom. Several organizations **are** interested in the SIN issue. During the past year, we sent background information to the Regional Municipality of Waterloo, the Ontario Ministry of Revenue, the Universities of Saskatchewan and Quebec, Nova Corporation and Maritime Telegraph and Telephone Company Ltd.

And there are kudos for the Quebec access and privacy commissioner's office for investigating SIN abuses in Quebec government agencies. Unlike most provinces which avoid the issue because SIN is a federal number, the Quebec commission seized the initiative and intervened under its own access and privacy legislation. For example, Quebec no longer demands a SIN to get a fishing permit for provincially controlled areas. As well, the automobile insurance industry has informally agreed to stop forcing clients to provide their SIN.

And the Quebec commission is now examining other provincial uses of the SIN including:

- Hydro-Québec's authority to use the SIN to identify both employees and subscribers;
- the Université de Laval's collection of SIN from students; and
- SIN use by hospitals, nursing homes and housing authorities.

It is encouraging to find that the federal government's efforts have had some impact outside its immediate jurisdiction.

Despite efforts to fine-tune listings in the blue (government) pages of telephone directories, more than half of the calls on the national toll-free line are unrelated to access or privacy. The receptionist re-directed 9343 callers to Reference Canada, the federal government's central information service. The office will make another attempt now that Bell Canada and the government telephone authority are working to improve the blue pages.

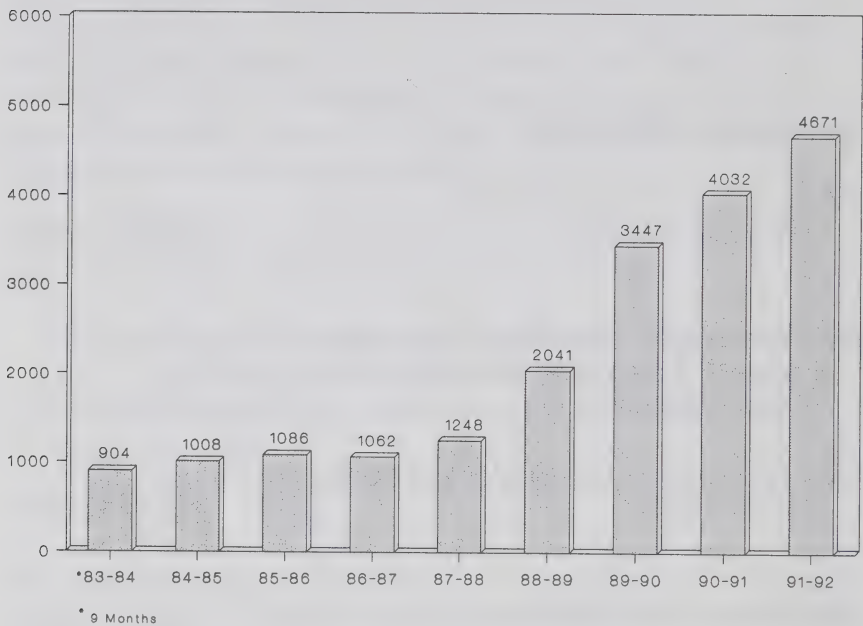
Finally, the office installed a device to communicate with callers with hearing or speech impediments (TDD).

The following two tables illustrate inquiries statistics. The first breaks out this year's inquiries by subject and the second compares numbers with previous years.

INQUIRIES 1991-92

What is the <i>Privacy Act</i> and How Can I Use It?	2420 (52%)
No Jurisdiction/Outside <i>Privacy Act</i> (Federal, Provincial, Municipal & Private Sectors)	808 (17%)
Use & Abuse of the Social Insurance Number (SIN)	588 (13%)
Misdirected Applications & Unrelated Matters	855 (18%)
TOTAL	4671

Inquiries 1983-92



Compliance Directorate

The directorate had two objectives for 1991-92. The first was to focus on a complex national organization—Canada Mortgage and Housing—with significant electronic data processing and communications components. Auditing CMHC permitted staff to examine distributed data processing and electronic communication issues and to further develop our EDP audit methodology.

The second objective was to review several smaller agencies dealing with women's and minority rights. Most of these organizations have large personal information collections, often because they investigate complaints. We selected Status of Women Canada, Canadian Advisory Council on the Status of Women, the Canadian Human Rights Commission and the Immigration and Refugee Board.

Audits were also completed on several other institutions such as National Defence, the National Capital Commission, Canadian Film Development Corporation, the Standards Council of Canada and various pilotage authorities. Work at 13 other organizations will carry over to 1992-93. Staff also

- investigated five incidents of lost or stolen files;
- audited three existing data-matches at Employment and Immigration Canada; and
- conducted a government-wide survey on the use of upward or reverse appraisals in federal institutions.

Trends and Problems

The past year's audits revealed some emerging trends in government information handling that demand attention. Foremost perhaps is the federal government's increasing use of private sector companies to provide services which handle personal information.

Contracting out—who's minding the data?

Budget pressures on government agencies have led many to use private industry for some of the services once performed in-house. For example, services such as Employee Assistance Programs, payroll applications and credit checking—and the personal information that goes with them—are now frequently handled by private companies under contract to the responsible government agencies.

The office has no quarrel with private companies performing services. However, unlike the federal government, the private sector is not covered by the *Privacy Act*. Thus, personal files handed over to private firms get no formal privacy protection unless specific clauses are written into the contracts. Since some departments use standard Supply and Services Canada contract forms and others draft their own, there is little consistency. Nevertheless, almost without exception, the contracts are deficient.

For example, contracts fail to:

- define ownership of the information;
- ensure employee access to the files;
- restrict further use of the personal data;
- protect against unauthorized disclosure;
- ensure proper disposal of files at contract end;
- establish retention and disposal criteria; and
- ensure the department's ability to audit compliance.

Our office is now working with Supply and Services Canada and Treasury Board to develop a standard contract. This should remedy many of the problems.

Checking employee credit ratings

Compliance auditors have found collection problems during examinations of personnel files. All permanent government employees—and many of those transferred or promoted—must undergo reliability checks. The department or agency obtains candidates' permission to check their credit ratings. Ratings are a combination of letters and numbers which describe the person's relative debt load and repayment behaviour.

The staff also found many of the same contracting problems described earlier. However, the credit checking process revealed other potential problems. For example, such large organizations as the RCMP, Canada Mortgage and Housing and National Defence often have direct on-line access to credit bureaus, allowing them to obtain substantially more personal financial data than a simple credit rating. There appears to be potential for abuse and nothing to prevent institutions from going on fishing expeditions.

In fact, most audited institutions tended to collect much more financial information than they needed. Details such as credit limits and account balances were found in files where only a simple credit rating was required. As well, the staff found credit reports containing not only the employee's information but also data on spouses. Credit bureaus often send out a work history and credit rating on the spouse, linking the information with the employee by Social Insurance Numbers and dates of birth.

Once in the hands of the government agency, credit information is often not kept secure. In some instances privacy staff found the information was transmitted by fax. In others, it was stored on the hard disk of desktop computers without adequate security protection.

Finally, much credit information is unreliable and therefore government institutions may be relying on incorrect data. Independent studies reveal a high error rate in credit files. Updates and corrections are made slowly and—sometimes—not at all. The onus rests entirely with individuals, even though stores and banks transmit the information to the credit bureaus.

Electronic transmission of personal information

Privacy audits have also found that government institutions routinely fax personal information. This courts the risks of having the transmission intercepted or sent to the wrong location. For example, an employee at the Canada Employment Centre in Sarnia, Ontario, sent four individuals' unemployment insurance queries to the local newspaper instead of the Employment and Immigration Canada office in London, Ontario. The employee had mistakenly punched the adjacent speed dial button which was programmed with the newspaper's number.

The incident was simple human error but it demonstrated the possible consequences of faxing personal information—a procedure auditors found in almost every institution visited. Fax is one type of technology where policies and procedures are not keeping pace. Little thought is given to what information should or should not be sent by fax. Employees transmit personal information from the most innocuous (lists of participants at meetings) to the most sensitive (medical records and credit checks).

Similar difficulties arise with the new electronic mail (E-mail) systems now being widely implemented. E-mail programs allow users of computer networks to communicate and transfer data within the network. Yet there are few policies or procedures to ensure that the data are shared only with those who need to know, or that it all remains secure.

Who's minding the computer?

One disturbing trend is that government seems not to be applying the same standards of management and control to its EDP resources as it does its paper records. Large complex government institutions appear not to know what hardware and software they own, let alone who has access and how the systems are being used. Increasingly, major collections of personal records are being automated but without formal controls. Electronic files lend themselves easily to improper collection, use and disclosure but, because the data are out of sight, they appear to be out of mind.

Portable computers: Automation of the federal government has seen the computer shrink from yesterday's roomful of equipment to today's notebook-sized units (with as much or more power) tucked into a briefcase. And already being tested is integrated chip technology which makes the plastic card "smart"—a mini-computer capable of storing and processing information.

However, these personal computing devices demand new management and control systems. Users often forget that these are not merely miniature typewriters. Computers remember what they process. Their loss or theft means not only lost valuable equipment but also lost information.

The office investigation this year of the theft of a personal computer from the Montreal office of Veterans Affairs illustrates the seriousness of such an incident. The computer was part of a new system on trial. It had been loaded with tombstone data on the office's entire 20,000 client base. Fortunately the personal details were very limited and the Commissioner decided not to notify the individuals concerned.

The investigation made it clear that Veterans Affairs staff had not followed the department's procedures for protecting valuable property. More important, however, investigators found no policies and procedures covering the storage and protection of the personal data in the computer memory. The Commissioner recommended that Veterans Affairs develop those policies and consider restricting storage of personal data to diskettes which could be removed and stored separately. Alternatively, personal data on personal computers could be encrypted to make it inaccessible to unauthorized users.

Controlling access in networks: The marriage of microcomputers and local or wide area networks poses another privacy challenge: determining which users should have access to what data. Auditors often find that authorized system users frequently can access information they do not need. The physical premises and the computer system may be secure from external threats but, once into the system, authorized users may access any data. Systems are needed to restrict users to the information they need to know.

Ending the pack rat syndrome: Auditors find few retention and disposal schedules for EDP files and those that do exist often do not correspond to the schedules for the paper files. Government may be shredding its paper but much of that paper was generated electronically. The data are replicated on hard and soft disks that seem to be kept indefinitely. Government agencies managing the retention and disposal of personal files need also to examine the electronic versions.

Describing information holdings

The description of government information holdings in *Info Source* continues to concern the Commissioner. Lack of resources may be a contributing factor but auditors find that *Info Source* is an incomplete and sometimes inaccurate catalogue of personal information held by government institutions. Some departments seem not to have a clear understanding of what they should list or how to change listings.

A common problem is the failure to list such federal employee standard banks as leave and attendance, travel and relocation, and training and development. The reverse is sometimes true—standard banks are listed but the institution holds no information. In fact, the bank is empty. And occasionally auditors and complaints investigators stumble upon information that seems not to be listed at all.

It may be time for Treasury Board to set out more clearly what institutions should describe and how to make changes. Also needed is a more rigorous review of the input government institutions provide to *Info Source*.

Upward appraisals

In earlier reports, the Privacy Commissioner expressed concern about the anonymity feature of upward or reverse appraisal processes being conducted in some departments. This process allows employees to rate and comment on their manager's performance, often anonymously.

In an effort to establish just how widespread the upward appraisal process has become and how it is being done, the Compliance Directorate polled 148 departments and agencies covered by the *Privacy Act*. At this writing it had received 141 responses (eight from one department), 27 of which were using or planning to use the process within the next 12 months. Of these 27, 24 promise employees anonymity and 18 use private consultants to analyze the results.

So fewer than 20 per cent of government agencies have embraced the idea. Nevertheless, one questions Canada's public service lending itself to a personnel relations process which relies upon the use of anonymous informants.

Corporate Management Branch

Corporate Management provides both the Privacy and Information Commissioners' offices with financial, administrative, informatics and library services.

The following are the offices' expenditures for the period April 1, 1991, to March 31, 1992.*

	Information	Privacy	Corporate Management	Total
Salaries	1,670,069	1,911,442	658,825	4,240,336
Employee Benefit Plan Contributions	285,600	307,020	121,380	714,000
Transportation and Communication	75,621	59,500	124,875	259,996
Information	21,005	55,261	3,109	79,375
Professional and Special Services	209,028	190,237	81,059	480,324
Rentals	4,391	3,276	11,945	19,612
Purchased Repair and Maintenance	6,688	6,358	7,199	20,245
Utilities, Materials and Supplies	18,692	9,814	29,070	57,576
Acquisition of Machinery and Equipment	109,474	44,361	12,959	166,794
Other Payments	2,970	1,873	250	5,093
TOTAL	2,403,538	2,589,142	1,050,671	6,043,351

* Expenditure figures do not incorporate final year-end adjustments reflected in the offices' 1991-92 Public Accounts.

Finance

The offices' total resources for the 1991-92 fiscal year were \$6,691,000 and 82 person-years, an increase of \$367,000 and four person-years over 1990-91. Personnel costs of \$4,954,336 and professional and special services expenditures of \$480,324 accounted for more than 90 per cent of expenditures. The remaining \$608,691 covered all other expenses.

Personnel

In the spirit of PS 2000, the unit made several improvements to the offices' personnel management practices by recruiting a management trainee, developing incentive awards and an orientation program for new employees, and streamlining some of its personnel procedures. In addition, the unit conducted a triennial classification audit, followed up the 1987 official languages audit and signed a letter of understanding on official languages with the Treasury Board.

Administration

The unit made continued progress on a retention and disposal schedule for records and also on an automated inventory of assets. As well, it evaluated the offices' telephone system to improve service to the public.

Informatics

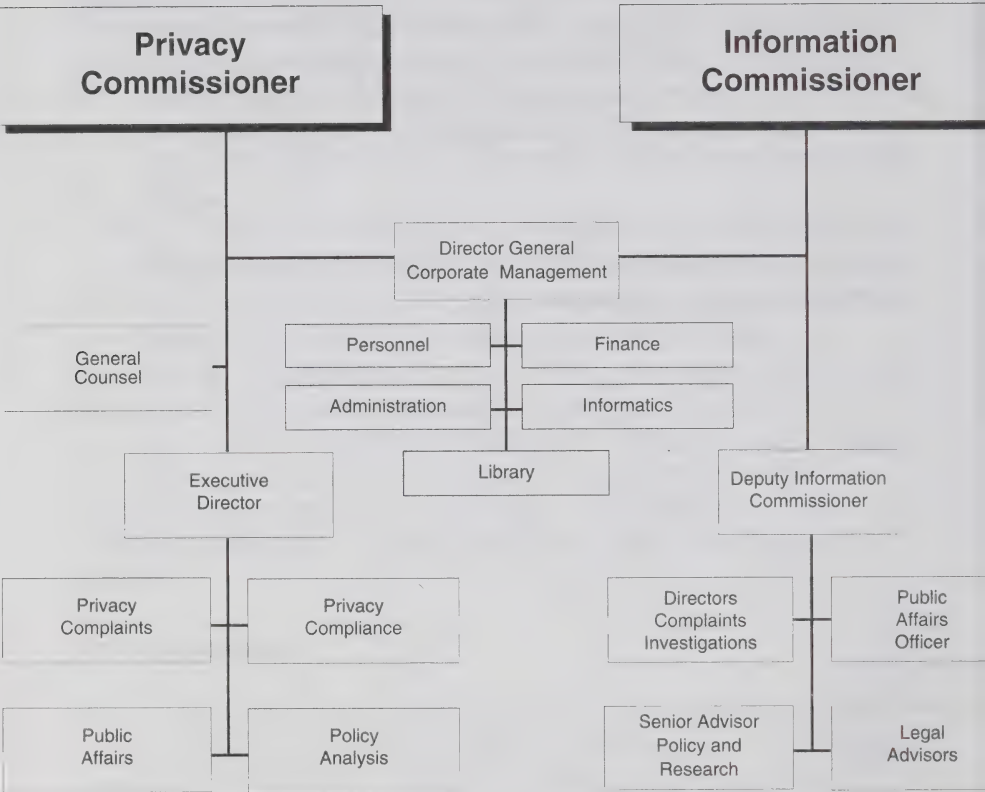
This year the unit completed three studies for a new case management system, office automation and using a computer network in a secure environment.

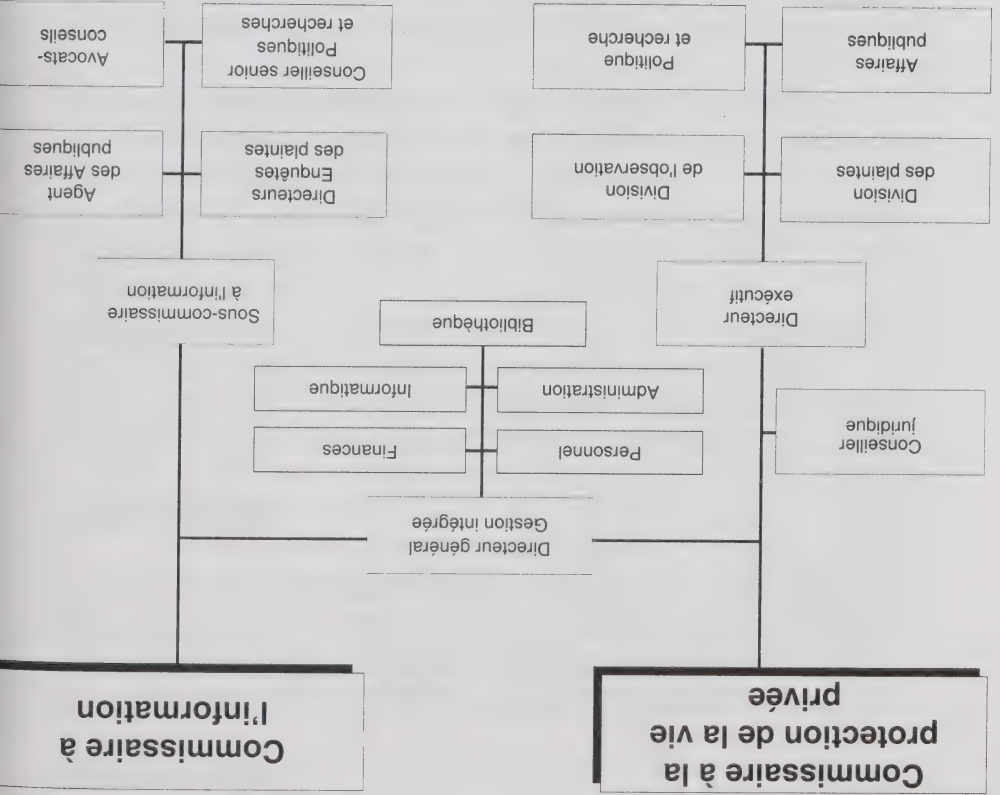
Library

The library provides interlibrary loan services, manual and automated reference and research, and subject-oriented media monitoring files. In addition to acquiring information on freedom of information, the right to privacy, data protection and the ombudsman function, the library has a special collection of Canadian and international ombudsmen's reports and departmental annual reports on the administration of the two acts.

The library (which is open to the public) handled 1,298 publication requests and answered 1,084 reference questions during the year.

Organization Chart





Informatique

Cette année, ce service a réalisé des études relativement à l'élaboration d'un nouveau système de gestion des cas, à la bureautique et à la mise en place d'un réseau informatique dans un contexte sécuritaire.

Bibliothèque

Les attributions de la bibliothèque concernent: les prêts entre bibliothèques; la documentation; les recherches manuelles et informatisées, ainsi que des dossiers thématiques de coupures de presse. La bibliothèque acquiert des ouvrages sur la liberté d'accès à l'information, le droit à la vie privée, la protection des données et la fonction d'ombudsman. Elle possède en outre une collection spéciale de rapports d'ombudsmans canadiens et étrangers ainsi que des rapports des ministères sur l'application des deux lois.

Au cours de l'année, la bibliothèque (qui est ouverte au public) a traité 1 298 demandes de prêts et a répondu à 1 084 questions à caractère documentaire.

Finances

Pour l'exercice financier 1991-1992, les ressources des commissariats ont totalisé 6 691 000 \$ et 82

années-personnes, soit une augmentation de 367 000 \$ et de quatre années-personnes par rapport à 1990-1991. Les dépenses au titre du personnel (4 954 336 \$) ainsi que les services professionnels et spéciaux (480 324 \$) représentent plus de 90 p. 100 des sommes globales. Les 608 691 \$ qui restent ont servi à couvrir les autres frais.

Personnel

Dans le sillage de FP 2000, les services du personnel ont apporté plusieurs améliorations à leurs méthodes de gestion: recrutement d'une stagiaire en gestion, élaboration d'un programme de primes à l'initiative et d'un programme d'orientation pour les nouveaux employés et rationalisation de certaines procédures. De plus, les responsables du personnel ont effectué une vérification triennale de la classification, ont assuré le suivi de la vérification de 1987 sur les langues officielles et ont signé un protocole d'entente avec le Conseil du Trésor en matière de langues officielles.

Administration

Les services d'administration ont continué d'avancer dans l'application du calendrier de conservation et d'élimination des documents et dans l'élaboration d'un répertoire informatisé des biens. De plus, le système téléphonique des commissariats a été évalué dans le but d'améliorer le service au public.

Gestion intégrée

La gestion intégrée assure à la fois au Commissariat à l'information et au Commissariat à la protection de la vie privée des services en matière de finances, de gestion du personnel, d'administration, d'informatique et de bibliothèque.

Ci-dessous les dépenses des commissariats pour la période allant du 1er avril 1991 au 31 mars 1992. *

	Information	Vie privée	Gestion intégrée	Total
Salaires	1 670 069	1 911 442	658 825	4 240 336
Contributions aux régimes d'avantages sociaux des employés	285 600	307 020	121 380	714 000
Transports et communications	75 621	59 500	124 875	259 996
Information	21 005	55 261	3 109	79 375
Services professionnels et spéciaux	209 028	190 237	81 059	480 324
Locations	4 391	3 276	11 945	19 612
Achats de services de réparation et d'entretien	6 688	6 358	7 199	20 245
Services publics, fournitures et approvisionnements	18 692	9 814	29 070	57 576
Acquisition de machines et d'équipement	109 474	44 361	12 959	166 794
Autres dépenses	2 970	1 873	250	5 093
TOTAL	2 403 538	2 589 142	1 050 671	6 043 351

Les dépenses n'incluent pas les ajustements de fin d'année reflétés dans la section des comptes publics 1991-1992 traitant des commissariats.

Dans des rapports annuels antérieurs, le Commissaire a exprimé des réserves quant à l'anonymat des évaluateurs qui faisaient des évaluations vers le haut dans certains ministères. Cette façon de procéder La donne aux fonctionnaires l'occasion d'évaluer le rendement de leurs supérieurs et de faire des commentaires à cet égard, souvent à titre anonyme.

Afin de déterminer à quel point ce procédé est répandu et comment il se déroule, la Direction de l'observation a fait un sondage auprès de 148 ministères et organismes assujettis à la *Loi sur la protection des renseignements personnels*. Au moment d'aller sous presse, le personnel de la Direction avait reçu 141 réponses, (dont 8 provenant d'un même ministère); 27 des ministères et organismes répondants ont dit avoir déjà recours à ce procédé ou prévoir s'en servir au cours des 12 prochains mois. Sur les 27, 24 ont promis de protéger l'anonymat des fonctionnaires évaluateurs et 18 emploient ou comptent employer des consultants du secteur privé pour l'analyse des résultats.

Bref, moins de vingt pourcent des organismes gouvernementaux ont retenu l'idée. Néanmoins, nous pouvons nous demander pourquoi l'administration fédérale devrait avoir recours à une procédure de relations du travail fondée comme celle-là sur le recours à des informateurs anonymes.

Description des renseignements détenus par l'administration fédérale

La description qu'*Info Source* donne des renseignements détenus par l'administration fédérale continue à préoccuper le Commissaire. Il est possible que le manque de ressources ait contribué à la situation, mais il n'empêche que les vérificateurs du Commissariat ont bien dû constater qu'*Info Source* est un répertoire incomplet - et parfois inexact - des renseignements personnels détenus par les institutions gouvernementales. Certains ministères ne semblent pas comprendre clairement ce qu'ils devraient inscrire au répertoire, ou comment changer leurs inscriptions. Par exemple, les ministères et organismes oublient souvent de mentionner dans le répertoire des banques de données aussi communes sur les fonctionnaires fédéraux que les registres des congés et des présences, ceux des voyages et des réinstallations et enfin ceux des cours de formation et de perfectionnement. Parfois, c'est l'inverse qui se passe : les banques de données figurent au répertoire, alors que l'institution ne détient aucun renseignement correspondant; en fait, les banques sont vides. Enfin, il arrive parfois, au gré des vérifications et des enquêtes sur les plaintes, qu'on découvre des renseignements ne figurant pas du tout au répertoire.

Le moment est peut-être venu pour que le Conseil du Trésor précise mieux les renseignements que les institutions devraient décrire et la façon de changer leurs inscriptions. Il faut aussi qu'on examine de façon plus rigoureuse les renseignements que les institutions gouvernementales communiquent à *Info Source*.

Contrôle de l'accès aux réseaux : La combinaison des micro-ordinateurs dans des réseaux locaux ou de plus grande envergure encore représente un nouveau défi pour la protection de la vie privée, celui de déterminer quels utilisateurs devraient avoir accès à quels renseignements. Les vérificateurs du Commissariat constatent souvent que les utilisateurs autorisés des systèmes peuvent fréquemment avoir accès à des renseignements dont ils n'ont pas besoin. Même si les locaux et le matériel informatique sont protégés contre des interventions de l'extérieur, une fois en communication avec le système, les utilisateurs peuvent avoir accès à toutes les données. Il faut qu'on mette au point des systèmes permettant d'empêcher les utilisateurs d'avoir accès à d'autres renseignements que ceux dont ils ont besoin.

Élimination du syndrome de l'écureuil : Les

vérificateurs ont constaté qu'il y a très peu de protocoles sur la durée de conservation et le calendrier de retrait des fichiers informatiques, et que, lorsqu'il y en a, les délais sont rarement les mêmes que ceux qui sont prévus pour les dossiers sur papier. L'administration gouvernementale détruit peut-être ses documents de papier, mais une grande partie sont générés électroniquement et reproduits sur des disques rigides ou des disquettes qui semblent être conservés indéfiniment. Par conséquent, les organismes gouvernementaux chargés de conserver et de retirer les dossiers personnels ont intérêt à ne pas négliger non plus leurs versions électroniques.

Les ordinateurs personnels perfectionnés nécessitent toutefois de nouveaux systèmes de gestion et de contrôle, car les utilisateurs oublient souvent qu'ils sont bien plus que des machines à écrire miniatures. En effet, comme l'ordinateur se souvient de ce qu'il a traité, lorsqu'il est perdu ou volé, tous les renseignements qu'il contient disparaissent avec lui.

Cette année, le Commissariat a dû enquêter sur le vol d'un ordinateur personnel dans les bureaux de Montréal du ministère des Anciens combattants. L'incident témoigne bien de toute la gravité d'une perte comme celle-là. L'ordinateur était utilisé pour les essais d'un nouveau système; on y avait stocké des données sur les pierres tombales de toute la clientèle régionale, soit quelque 20 000 personnes. Heureusement, les renseignements personnels en question étaient très limités, de sorte que le Commissaire a décidé de ne pas informer les intéressés du vol.

L'enquête a révélé que le personnel des Anciens combattants n'avait pas respecté la procédure ministérielle de protection des biens de valeur. Mais il y a pire. Les enquêteurs ont constaté que le ministère n'avait pas de politique ou de procédure sur la conservation et la protection des renseignements personnels stockés sur ordinateur. Le Commissaire a donc recommandé aux Anciens combattants de se donner la politique voulue et d'envisager de stocker les renseignements personnels seulement sur des disquettes pouvant être retirées des ordinateurs et conservées à part. Il a aussi proposé une solution de rechange, le codage des renseignements personnels conservés sur ordinateur pour les rendre inaccessibles aux utilisateurs n'ayant pas les autorisations nécessaires.

Qui surveille l'ordinateur?

Une tendance inquiétante se dessine : l'administration gouvernementale ne semble pas avoir les mêmes normes de gestion et de contrôle pour ses fichiers informatiques que pour ses dossiers sur papier. De grandes institutions gouvernementales complexes donnent l'impression de ne pas savoir de quels matériels elles disposent et quels logiciels elles emploient, et encore moins avoir une idée de ceux qui ont accès à leurs systèmes informatiques et de la façon dont ils sont utilisés. Des collections de plus en plus importantes de fichiers de données personnelles sont automatisées, mais les contrôles nécessaires manquent. Dans le cas de données informatisées, parce que celles-ci n'occupent pas un espace défini, on a tendance à en négliger la sécurité.

Ordinateurs portatifs : l'administration fédérale s'est automatisée en même temps qu'on miniaturisait l'ordinateur. Aujourd'hui, des appareils au moins aussi puissants que ceux qui occupaient naguère toute une pièce sont de la taille d'un bloc-notes et tiennent facilement dans un porte-documents. Et ce n'est pas fini : la technologie des puces à circuits intégrés est déjà à l'essai, et elle a rendu possible les cartes à mémoire en plastique, c'est-à-dire de minuscules ordinateurs capables de mémoriser et de traiter des données.

Cette erreur humaine est un bon exemple des conséquences de la transmission de renseignements personnels par télécopieur. Malheureusement, les vérificateurs ont constaté l'existence de cette pratique dans presque toutes les institutions visitées. Dans ce domaine, les politiques et procédures n'évoluent pas au rythme de la technologie. On se pose très peu de question sur le genre d'information dont on devrait autoriser ou interdire la transmission par télécopieur. Bref, les fonctionnaires transmettent toutes sortes de renseignements personnels, des plus banales (listes de participants à des réunions) aux plus délicats (dossiers médicaux et vérifications de crédit).

Le même raisonnement s'applique aux nouveaux systèmes de courrier électronique, qui sont de plus en plus répandus. Les programmes de courrier électronique conçus à cette fin permettent aux utilisateurs des réseaux d'ordinateurs de communiquer et de transférer des données partout dans les réseaux auxquels ils sont reliés. Pourtant, dans ce contexte, il n'existe à peu près pas de politiques ou de procédures servant à assurer la protection des données ou à faire en sorte qu'elles ne soient communiquées qu'à ceux qui ont besoin de savoir.

Les vérifications ont révélé que les institutions gouvernementales se servent régulièrement de télécopieurs pour envoyer ou recevoir des renseignements personnels. Les transmissions peuvent être interceptées, ou transmises au mauvais numéro. C'est ainsi qu'un fonctionnaire travaillant au Centre d'emploi du Canada à Sarnia, en Ontario, a envoyé des demandes de renseignements sur l'assurance-chômage de quatre personnes au journal local plutôt qu'au bureau d'EIC de London. Il avait appuyé par erreur sur la mauvaise touche de composition rapide, qui correspondait au numéro du journal.

Transmissions électroniques des renseignements personnels

Enfin, une grande partie des renseignements sur le crédit des fonctionnaires ne sont pas fiables. Des études réalisées par des chercheurs indépendants ont révélé un pourcentage d'erreur élevé dans les dossiers de crédit. Les mises à jour et les corrections sont faites lentement... quand elles le sont. C'est toujours l'intéressé qui doit voir à ce que l'information soit exacte, même si ce sont les magasins et les banques qui la transmettent aux bureaux de crédit.

Pire, une fois que l'institution gouvernementale a ces renseignements sur le crédit, il arrive souvent qu'elle ne les protège pas convenablement. Dans certains cas, le personnel du Commissariat a constaté que l'on avait télécopié ces renseignements. Dans d'autres cas, ils avaient été stockés dans des disques rigides d'ordinateurs de bureaux, sans protection suffisante.

Le personnel du Commissariat a relevé là une grande partie des problèmes constatés dans le cas des contrats, mais, dans le cas des vérifications de crédit, il y en a d'autres. Par exemple, les ministères et organismes ayant un effectif important, comme la GRC, la SCHL et le MDN, sont souvent reliés en direct aux ordinateurs des bureaux de crédit, ce qui leur permet d'en tirer nettement plus de données financières personnelles que s'ils demandaient une simple cote de crédit. Les risques d'abus sont évidents, et rien n'empêche les institutions fédérales de chercher à obtenir des renseignements qui ne les concernent pas.

En fait, la plupart des institutions qui ont fait l'objet d'une vérification par le Commissariat tendent à recueillir beaucoup plus de renseignements financiers qu'elles n'en ont besoin. Les enquêteurs ont trouvé dans les dossiers des détails tels que des marges de crédit et des soldes bancaires, là où, une simple cote de crédit aurait suffi. De plus, certains rapports de crédit contenaient des renseignements non seulement sur le fonctionnaire visé, mais aussi sur son conjoint ou sa conjointe. Les bureaux de crédit établissent souvent un relevé des antécédents professionnels et de la cote de crédit du conjoint ou de la conjointe et les annexent aux renseignements concernant l'intéressé, en se servant des numéros d'assurance sociale et des dates de naissance.

- les critères de conservation et de retrait ne sont pas précisés; et
- rien n'est prévu pour assurer la capacité du ministère (ou de l'organisme) à vérifier si les règles sont respectées.

Le Commissariat collabore actuellement avec Approvisionnement et Services Canada et avec le Conseil du Trésor en vue de rédiger un contrat normalisé qui devrait remédier à presque tous ces problèmes.

Vérification de la cote de crédit des employés

Les vérificateurs du Commissariat ont aussi constaté des problèmes de surcollecte de renseignements au cours de leur examen des dossiers du personnel. En effet, tous les fonctionnaires nommés pour une période indéterminée - et une grande partie de ceux qui sont mutés ou promus - doivent faire l'objet d'une vérification dite de fiabilité. Le ministère ou l'organisme employeur obtient leur autorisation de vérifier leur cote de crédit auprès des bureaux de crédit locaux. Les cotes de crédit sont une combinaison de lettres et de chiffres qui décrivent l'endettement relatif de l'intéressé et son comportement de débiteur.

- Le Commissariat n'a aucune objection à ce que des entreprises privées offrent des services à l'administration fédérale; toutefois, contrairement à celle-ci, ces entreprises ne sont pas assujetties à la *Loi sur la protection des renseignements personnels*. Par conséquent, les dossiers personnels transférés à l'entreprise privée ne bénéficient plus de la moindre protection légale des renseignements qu'ils recèlent, à moins que les contrats passés entre les organismes gouvernementaux et les fournisseurs ne contiennent de clauses expresses à ce sujet. Étant donné que certains ministères et organismes utilisent les formulaires de contrat normalisés d'Approvisionnements et Services Canada alors que d'autres préfèrent les leurs, le manque d'uniformité est la règle plutôt que l'exception. Presque tous les contrats analysés présentaient des lacunes.
- Ces lacunes sont les suivantes :
- la propriété des renseignements n'est pas définie;
 - l'accès des employés aux dossiers n'est pas assuré;
 - l'utilisation ultérieure des renseignements personnels n'est pas limitée;
 - il n'y a aucune protection contre la communication non autorisée des renseignements;
 - il n'y a pas de dispositions propres à assurer le retrait des dossiers conformément aux règles à l'expiration du contrat;

Les contraintes budgétaires imposées aux organismes gouvernementaux en ont incité beaucoup à chercher dans l'entreprise privée certains services naguère internes. Par exemple, des services comme les programmes d'aide aux employés, la gestion des listes de paye et les vérifications de crédit - avec les renseignements personnels nécessaires dans chaque cas - sont maintenant fréquemment confiés à contrat à des entreprises privées.

Contrats accordés à l'extérieur - qui surveille?

Les vérifications réalisées au cours de la dernière année ont révélé des tendances qu'il ne faudrait pas négliger sur la façon de traiter l'information dans l'administration fédérale. La plus manifeste de ces tendances est sans doute le recours croissant de la Fonction publique à des entreprises privées de services et notamment de traitement des renseignements personnels.

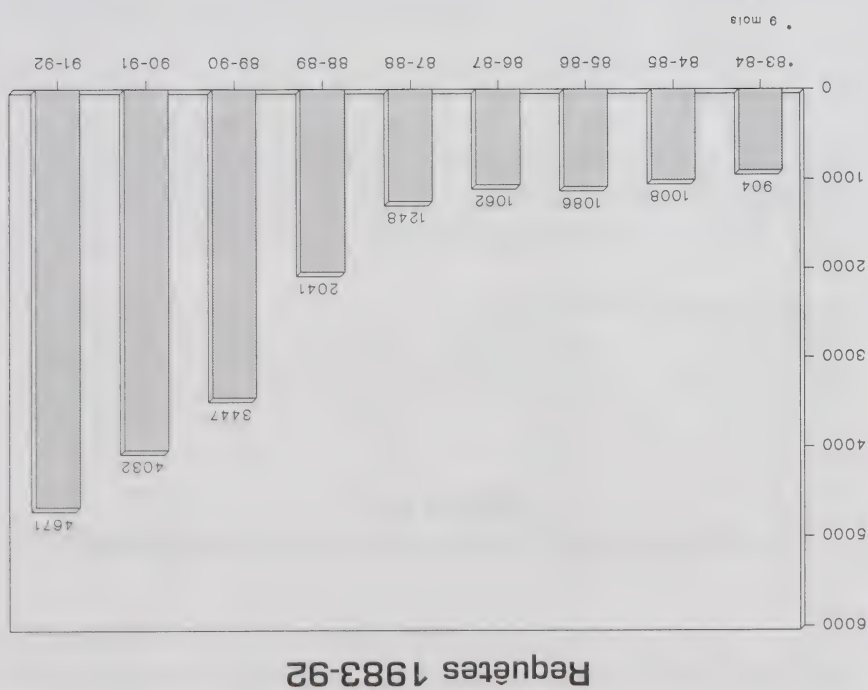
Tendances et problèmes

- enquête sur cinq cas de fichiers perdus ou volés;
- effectuée la vérification de trois coupages de données existants à Emploi et Immigration Canada; et
- réalisé un sondage à l'échelle de toute l'administration fédérale sur l'utilisation des évaluations vers le haut (inversées) dans les institutions fédérales.

La Direction avait deux objectifs en 1991-1992. Le premier consistait à concentrer ses travaux de vérification sur un organisme national complexe, la Société canadienne d'hypothèques et de logement (SCHL), qui a d'importants volets de traitement électronique des données et de communications. La vérification des activités de la SCHL a donné au personnel l'occasion d'étudier le traitement des données distribuées et les questions de communications électroniques, ainsi que de perfectionner sa méthode de vérification du TED.

Le deuxième objectif de la Direction consistait à faire des vérifications dans plusieurs petits organismes du secteur des droits des femmes et des minorités. La plupart de ces organismes ont d'importantes collections de renseignements personnels, souvent parce qu'ils instruisent des plaintes. Ceux qui ont fait l'objet d'une vérification au cours de la dernière année sont Condition féminine Canada, le Conseil consultatif canadien sur la situation de la femme, la Commission canadienne des droits de la personne et la Commission de l'immigration et du statut de réfugié.

Le personnel de la Direction a aussi terminé ses travaux de vérification au ministère de la Défense nationale, à la Commission de la Capitale nationale, à la Société d'expansion de l'industrie cinématographique canadienne, au Conseil canadien des normes et à diverses commissions de pilotage. Les travaux de vérification entrepris dans treize autres organismes se prolongeront en 1992-1993. Le personnel a aussi



Les deux tableaux suivants illustrent les statistiques des demandes de renseignements. Le premier compare les nombres de demandes avec ceux des années précédentes; le second est une ventilation par sujet des demandes de l'année écoulée.

DEMANDES DE RENSEIGNEMENTS REÇUES 1991-1992

Qu'est-ce que la Loi sur la protection des renseignements personnels et comment puis-je m'en prévaloir?	2 420 (52 %)
Questions échappant à la compétence du Commissariat/à la Loi sur la protection des renseignements personnels (secteurs fédéral, provincial, municipal et privé)	808 (17 %)
Utilisation justifiée ou abusive du numéro d'assurance sociale (NAS)	588 (13 %)
Demandes au mauvais organisme et questions n'ayant rien à voir avec la Loi sur la protection des renseignements personnels	855 (18 %)
TOTAL.....	4 671

Enfin, le Commissariat a installé cette année un dispositif de communication pour les correspondants souffrant de troubles de l'ouïe et de la parole (ATS).

Cela dit, en dépit des efforts que le Commissariat a déployés pour clarifier son inscription dans les pages bleues (organismes gouvernementaux) des boîtins téléphoniques, plus de la moitié des appels qu'il reçoit sur sa ligne 800 accessible de tous les coins du pays n'ont rien à voir avec l'accès à l'information ou la protection des renseignements personnels. La réceptionniste a dû aiguiller 9 343 correspondants vers Référence Canada, le service central d'information de l'administration fédérale. Le Commissariat tentera une fois de plus de remédier à ce problème maintenant que Bell Canada et les services gouvernementaux responsables du téléphone se donnent la main pour améliorer les pages bleues.

En outre, la Commission québécoise d'accès à l'information et de protection de la vie privée mérite des éloges pour ses enquêtes sur les utilisations abusives du NAS dans les organismes gouvernementaux du Québec. Contrairement à la plupart des provinces qui éludent la question parce que le NAS est un numéro d'identification fédéral, la Commission québécoise a saisi l'initiative et elle est intervenue en vertu de sa propre loi sur l'accès à l'information et sur la protection de la vie privée. Résultat? Le Québec n'exige plus qu'on produise son NAS pour obtenir un permis de pêche dans les zones de compétence provinciale. De même, l'industrie de l'assurance-automobile a consenti tacitement à ne plus obliger ses clients à lui fournir leur NAS.

Loin de s'arrêter là, la Commission québécoise enquête actuellement sur d'autres utilisations provinciales du NAS :

- le droit d'Hydro-Québec d'utiliser le NAS pour identifier tant ses employés que ses abonnés;
- la pratique de l'Université Laval d'exiger le NAS de ses étudiants; et
- l'utilisation du NAS par les hôpitaux, notamment pour malades chroniques, les maisons de convalescence et les organismes de logement.

Où, il est vraiment encourageant de constater que les efforts du gouvernement fédéral ont eu une certaine influence au-delà de son propre secteur de compétence.

Les agents du Commissariat chargés des demandes de renseignements passent une grande partie de leur temps à expliquer les mesures limitées de contrôle de l'utilisation des numéros d'assurance sociale (NAS). La plupart des gens croient que l'utilisation du NAS a été limitée par la législation qui a créé les régimes d'assurance-chômage et de pensions, dans les années soixante. Or, en dépit des promesses qui avaient été faites à l'époque, ce n'est pas le cas. Un grand nombre de nos correspondants ont du mal à accepter l'idée que seul le gouvernement fédéral limite son utilisation du NAS.

Trop souvent hélas, les gens doivent choisir entre la protection de leur NAS et l'obtention des biens et des services qu'ils veulent. Vu que le mandat du Commissariat est limité, le personnel encourage maintenant les correspondants à écrire à leurs députés, dans l'espoir que, si plus de députés reçoivent des plaintes, ils pourraient être incités à agir pour contrôler les utilisations abusives du NAS.

Et pourtant, tout n'est pas perdu. Plusieurs organisations s'intéressent à cette question. Au cours de la dernière année, le Commissariat a envoyé de la documentation à la Municipalité régionale de Waterloo, au ministère du Revenu de l'Ontario, aux universités de la Saskatchewan et du Québec, à Nova Corporation et à Maritime Telegraph & Telephone.

Il reste que les correspondants du Commissariat sont toujours étouffés de constater l'absence totale de réglementation dans le secteur privé. Les nombreux appels de personnes qui ont des difficultés à consulter ou à protéger les renseignements personnels qui les concernent et que détiennent des organisations privées en témoignent. Il est frustrant pour le Commissariat de devoir avouer qu'il n'y peut rien, puisque sa compétence se limite à l'administration fédérale. Pire encore, il est incapable de proposer à ses correspondants des moyens de régler leurs problèmes.

Bien que la *Loi sur la protection des renseignements personnels* soit une loi fédérale, des certaines d'organismes et d'entreprises réglementées par l'administration fédérale lui échappent, notamment les Chemins de fer nationaux du Canada, Via Rail, Air Canada, Énergie atomique du Canada Limitée, diverses corporations de ports, ainsi que des compagnies de téléphone et des institutions financières comme les banques et les compagnies d'assurance.

Le Commissariat a aussi répondu à des appels sur la façon de traiter les renseignements personnels dans les bureaux des députés ainsi qu'à la Commission royale sur les nouvelles techniques de reproduction. Les employés et les clients sont effarés d'apprendre que nous ne pouvons pas intervenir et qu'ils ne peuvent pas non plus invoquer les lois provinciales ou les règlements municipaux.

Le gouvernement du pays en question avait saisi le passeport et l'avait remis aux représentants des Affaires extérieures en partant du principe que, si le prévenu était bel et bien citoyen canadien, le Canada allait lui délivrer des documents de voyage à sa libération. Bien entendu, l'ambassade du Canada n'allait pas fournir de services consulaires ou des documents de voyage à un individu qui n'est pas Canadien.

Le Commissariat a reconnu que la divulgation était fondée, étant donné qu'il est d'intérêt public de protéger l'intégrité des passeports canadiens. En outre, il est important que les Canadiens ne soient pas alarmés par des rumeurs sur le refus de services consulaires à de prétendus «citoyens» du Canada.

Demandes de renseignements - Le public réagit

Les agents du Commissariat continuent à répondre à un nombre sans cesse croissant de lettres et d'appels téléphoniques : le Commissariat en a reçu 4 671 au cours de l'année écoulée. La ligne téléphonique (qu'il partage avec le Commissariat à l'information) permet aux Canadiens de l'appeler sans frais de tous les coins du pays et est le seul service national du genre d'accès à l'information et de protection de la vie privée.

Les Canadiens sont de plus en plus au courant des mesures existantes de protection de leur vie privée ainsi que des nouvelles lois ou dispositions législatives envisagées par les gouvernements provinciaux et par les autorités municipales. La Saskatchewan vient tout juste de proclamer sa loi (*Freedom of Information and Privacy Act*) et la Colombie-Britannique et l'Alberta ont toutes deux promis d'adopter des lois analogues dans leurs derniers discours du Trône.

Anciens combattants Canada a téléphoné au Commissariat au sujet de la demande. À la fin de la conversation, le ministère avait l'impression qu'il lui faudrait obtenir le consentement écrit de chacun des anciens combattants visés. [En fait, ce n'était là qu'une des avenues proposées par le Commissariat.] Ce message a été communiqué au personnel de la Chancellerie qui, dans un réflexe de frustration bien compréhensible, a téléphoné directement au Commissariat.

Le Commissariat a demandé à voir un avis écrit et un échantillon des renseignements que la Chancellerie voulait faire tirer de la base de données. L'examen de ces documents lui a permis de constater que toutes les personnes dont les noms figuraient sur la liste avaient manifesté de l'intérêt pour la médaille, de sorte que la divulgation des renseignements qui les concernaient allait être à leur avantage. D'autre part, le Commissariat a proposé à Anciens combattants Canada de demander à la Chancellerie de s'engager par écrit à n'utiliser les données que dans ce contexte, puis à les détruire ou à les lui retourner.

Le malentendu a vite été réglé et le Gouverneur général a décerné la première des médailles lors d'une cérémonie à Ottawa le 10 novembre 1991.

Une fausse déclaration de citoyenneté canadienne

Le ministère des Affaires extérieures a avisé le Commissaire de son intention d'informer le gouvernement d'un pays étranger qu'un individu arrêté sur le territoire de ce pays pour une affaire de drogue n'était pas citoyen du Canada, même s'il était porteur d'un passeport canadien.

Le MDN a communiqué le rapport d'autopsie au médecin, puis il en a informé le Commissaire. Normalement, le Commissariat préfère recevoir un préavis, mais le MDN avait reçu la demande de divulgation pendant la grève de la Fonction publique; il était alors sans personnel de bureau. Le Commissaire ne s'est pas opposé à la divulgation.

Liste d'anciens combattants de la guerre de Corée envoyée à Rideau Hall

Le Bureau du Gouverneur général a été la source d'une autre demande de renseignements personnels, au sujet cette fois d'anciens combattants de la guerre de Corée. L'affaire montre bien à quel point les malentendus sont faciles, lorsqu'on communique par téléphone.

La Chancellerie avait demandé à Anciens combattants Canada de lui donner accès à sa base de données de renseignements personnels sur les anciens combattants admissibles à la Médaille canadienne de service volontaire pour la Corée. La Chancellerie avait besoin de ces renseignements (noms et adresses, langue, numéro de service et confirmation d'admissibilité) pour pouvoir traiter plus vite les demandes d'obtention de cette nouvelle médaille de la guerre de Corée. Le Bureau du Gouverneur général voulait décerner les médailles en novembre 1991.

Une liste de pilotes et de mécaniciens n'a pas été divulguée

Le ministère de la Défense nationale (MDN) a demandé à Transports Canada de lui communiquer une liste de pilotes d'hélicoptères et de mécaniciens d'entretien de la région d'Ottawa, pour pouvoir les informer des possibilités d'emploi à la Défense.

Le Commissariat est rarement favorable à ce genre de divulgation d'une liste générale quand il y a d'autres moyens de communiquer avec les intéressés. La divulgation de la liste est peut-être à l'avantage que ceux qui décrochent des emplois, mais pas à celui des autres, en l'occurrence plusieurs centaines de personnes. Le Commissariat a donc proposé que Transports Canada envoie par la poste des avis pour le MDN, ou que le MDN place tout simplement des annonces dans les journaux locaux et dans les publications professionnelles.

Transports Canada a décidé de ne pas fournir la liste.

Divulcation d'un rapport d'autopsie à un médecin de famille

Un médecin a demandé au ministère de la Défense nationale de lui envoyer le rapport d'autopsie d'un membre des Forces canadiennes qui était mort subitement en faisant du jogging. Le médecin traitait un membre de la famille du militaire décédé et voulait savoir si l'officier souffrait de la même affection susceptible de contribuer à causer une crise cardiaque. Puisqu'on soupçonne que l'affection en question est héréditaire, le médecin voulait commencer immédiatement à traiter les autres membres de la famille du défunt.

Divulgations en vue de la remise d'une distinction pour bravoure

La GRC a avisé le Commissaire que la Direction des distinctions honorifiques de la Chancellerie (l'une des composantes du Bureau du Gouverneur général) lui avait demandé des renseignements sur l'une des victimes de l'écrasement d'un avion dans l'Arctique en 1972. La Chancellerie envisageait de décerner une distinction pour bravoure (à titre posthume) à un jeune Inuit qui avait survécu à l'écrasement et sauvé la vie du pilote blessé, mais qui était mort avant que les secours arrivent.

La Chancellerie remettait en question toute sa démarche par suite de la publication d'un deuxième livre sur l'accident dans lequel figuraient des détails sur le rôle joué par le jeune homme dans la survie du pilote.

L'enquêteur du Commissariat a étudié les documents que la GRC se proposait de divulguer et il a constaté qu'ils contenaient moins de renseignements personnels que la transcription de l'enquête du coroner ou que l'un ou l'autre des deux livres publiés sur l'écrasement de l'avion. Par ailleurs, les documents qui auraient été divulgués confirmaient l'exactitude de certains des détails du livre en question.

Le Commissariat ne s'est pas opposé à la divulgation, en concluant qu'on n'avait pas besoin d'en informer le seul survivant puisque les renseignements étaient déjà

publics.

Le rapport suggérerait que des copies des rapports soient mises à la disposition du Comité de la Justice et du Solliciteur général à l'occasion d'une séance à huit clos. Voici des exemples d'autres préavis reçus pour des raisons d'intérêt public.

La divulgation entraîne le dépôt d'une plainte au Commissaire

Le Bureau du Conseil privé (BCP) a avisé le Commissaire de son intention de divulguer des renseignements personnels concernant plusieurs personnes à un organisme professionnel qui enquêtait sur la conduite de deux de ses membres. Les documents avaient été déposés en preuve devant une commission fédérale d'enquête.

Le BCP avait obtenu le consentement d'un individu (qui n'était pas visé par une enquête), mais il ne jugeait pas pratique d'obtenir le consentement de tous les intéressés. Le Commissariat s'est dit d'avis que tous ces gens devaient être informés de la divulgation imminente des renseignements, en laissant entendre que l'avis risquerait moins de les perturber s'il émanait directement du BCP. Celui-ci a retenu la proposition et écrit à chacun des intéressés, en exposant les motifs de la divulgation et en citant la disposition pertinente de la Loi sur la protection des renseignements personnels. L'une des personnes en cause s'est opposée à la divulgation et a depuis porté plainte auprès du Commissaire à la protection de la vie privée.

L'an dernier, le Commissaire a souligné dans son rapport toute la difficulté de concilier la protection de la vie privée et l'intérêt public, dans le cas de la divulgation de rapports portant sur des évasions de prison au cours desquelles trois personnes avaient été assassinées (voir Rapport annuel 1990-1991).

Le Solliciteur général avait alors refusé de donner au Comité permanent de la Justice et du Solliciteur général les versions intégrales de ces rapports d'enquête, en déclarant que la *Loi sur la protection des renseignements personnels* en interdisait la divulgation.

Son refus avait fait l'objet d'une question de privilège à la Chambre des communes, et le Commissaire par intérim avait été appelé à témoigner devant le Comité permanent des privilèges et des élections, où il avait dit ne voir aucune difficulté à ce que le Solliciteur général communique la version intégrale des rapports au Comité, dans une séance à huit clos.

Le Comité des privilèges et des élections a conclu dans son rapport, "qu'aucune disposition de la *Loi sur la protection des renseignements personnels* n'empêche la Chambre des communes d'adopter un ordre exigeant la production des versions non expurgées des deux rapports. Par conséquent, nous ne croyons pas qu'il soit nécessaire ou souhaitable de modifier la *Loi sur la protection des renseignements personnels* afin de permettre la production de ces rapports".

Cette année, le Commissariat a reçu 43 préavis d'organismes gouvernementaux qui compartaient divulguer des renseignements personnels pour des raisons «d'intérêt public» ou à l'avantage de l'individu concerné. Dans ce contexte, le rôle du Commissaire se borne à informer les intéressés de la divulgation envisagée, s'il le juge bon. Il peut conseiller de ne pas divulguer les renseignements, mais il ne peut pas interdire de le faire.

Le personnel du Commissariat dépouille les préavis, de façon à ce que le Commissaire puisse étudier les plaintes qu'il pourrait recevoir à ce sujet sans avoir déjà jugé de l'opportunité de la divulgation.

L'alinéa 8(2)m) de la Loi est censé porter sur les divulgations de nature exceptionnelle, et pourtant, bien des préavis sont devenus si répétitifs qu'ils imposent une lourde charge administrative tant au ministère responsable qu'au Commissariat lui-même.

Par exemple, Multiculturalisme et Citoyenneté Canada envoie régulièrement un préavis de divulgation au Commissaire avant de confirmer le statut de citoyen canadien des personnes sélectionnées pour être nommées à l'Ordre du Canada. Etant donné qu'il s'agit là d'une utilisation courante de documents relatifs à la citoyenneté, le Commissariat a proposé au ministère de le faire savoir publiquement et de modifier en conséquence son inscription dans *Info Source*. Le ministère a retenu cette proposition, qui lui a permis d'éliminer de la paperasse dans ses opérations et de donner au public une idée plus claire de la façon dont les renseignements concernant la citoyenneté peuvent être utilisés.

L'enquête a confirmé que, depuis le 14 décembre 1983, il est convenu que tous les renseignements communiqués à Santé et Bien-être social par la Commission des accidents du travail de l'Ontario sont confidentiels et ne doivent pas être divulgués, sauf par la Commission elle-même.

Nonobstant cette entente, l'enquêteur du Commissariat a demandé à Santé et Bien-être social de demander à la direction de la Commission l'autorisation de communiquer les renseignements en question. Le ministère a bien voulu le faire, à la suite de quoi la Commission a modifié sa politique l'autorisant à communiquer les renseignements directement aux personnes qui en font la demande.

C'est un changement important de la politique qui devrait simplifier la procédure nécessaire pour bien des requérants.

Le Commissaire a conclu que la plainte n'était pas bien fondée, étant donné que Santé et Bien-être social n'avait pas auparavant le droit de divulguer les renseignements obtenus de la Commission. Il a applaudi à la décision de la Commission de modifier sa politique.

Les dossiers de la Commission des accidents du travail de l'Ontario ne sont plus «confidentiels»

Un avocat s'est plaint que Santé et Bien-être social Canada avait refusé de lui donner accès à 20 pages du dossier médical d'invalidité du Régime de pensions du Canada de son client, dossier provenant de la Commission des accidents du travail de l'Ontario.

À la suggestion de Santé et Bien-être social, l'avocat s'est adressé directement à la Commission, qui lui a envoyé plus de documents que le ministère ne lui en avait refusés, ce qui l'a laissé dans l'impossibilité de juger sur quels documents le ministère s'était fondé pour rejeter la demande de son client. L'avocat a déclaré qu'il lui serait impossible de représenter convenablement son client dans une procédure d'appel de pension s'il ne savait pas exactement quels documents le ministère avait reçus de la Commission.

L'enquêteur a constaté que Santé et Bien-être social avait refusé de communiquer 20 pages à l'avocat en invoquant l'alinéa 19(1)c) de la *Loi sur la protection des renseignements personnels*, qui enjoint aux institutions fédérales de refuser de communiquer des renseignements personnels qu'elles ont obtenus «à titre confidentiel» des gouvernements des provinces ou de leurs organismes. Il n'y a aucune possibilité d'interprétation et aucune latitude aux organismes fédéraux à cet égard.

Par conséquent, une fois qu'un gouvernement provincial ou une administration municipale déclare que des renseignements sont confidentiels, il est interdit aux organismes fédéraux de les divulguer, si banals soient-ils.

L'enquête du Commissaire a confirmé que Consommation et Affaires commerciales Canada avait refusé de communiquer des renseignements recueillis par son directeur des Enquêtes et Recherches, en disant qu'ils n'avaient été au cours d'une enquête légale. Étant donné que la direction générale en question est l'un des «organismes d'enquête» mentionnés dans la *Loi sur la protection des renseignements personnels*, l'alinéa 22(1)a) de la Loi l'autorise à refuser de communiquer les renseignements obtenus au cours de ses enquêtes.

Effectivement, comme les renseignements avaient été recueillis pendant que le directeur des Enquêtes et Recherches instruisait une plainte portée en vertu de la *Loi sur la concurrence*, le ministère avait le droit de refuser de les communiquer. Néanmoins, le Commissaire a déclaré que les renseignements en question étaient relativement anodins, et que la

plainte en connaissance probable déjà la teneur. Ses arguments et son raisonnement n'ont toutefois pas réussi à convaincre le ministère de communiquer les renseignements demandés. Le ministère a tenu à se prévaloir de son droit de refuser, même s'il était fort peu probable qu'il aurait nu à son enquête ou à qui que ce soit en communiquant les renseignements demandés au plaignant.

Étant donné que Consommation et Affaires commerciales Canada n'est pas tenu de démontrer qu'il y a un risque à communiquer les renseignements demandés, en vertu de l'alinéa 22(1)a), le Commissaire a été bien obligé de dire au plaignant que, même s'il n'était pas du tout d'accord avec le ministère sur ce point, celui-ci avait respecté la lettre de la loi. Autrement dit, il devait juger que la plainte n'était pas bien fondée.

Un homme d'Ottawa a demandé au Commissaire d'enquêter sur plusieurs plaintes qu'il avait portées contre Consommation et Affaires commerciales Canada (CCC), en disant que le ministère avait eu tort de lui refuser l'accès aux renseignements personnels qui le concernent. Le plaignant avait déjà porté plainte en vertu de la *Loi sur la concurrence*. Comme les résultats de l'enquête l'avaient laissé sur sa faim, il voulait avoir accès aux commentaires que le personnel du ministère avait faits à son sujet dans le dossier.

Le refus était légal mais inutile

Toutefois, il a pu rassurer le plaignant en lui disant que la Société canadienne des postes n'a plus ses empreintes digitales ni le double de son casier judiciaire, et que ces renseignements ont été bien protégés pendant le peu de temps qu'elle les a eus en sa possession. De plus, la GRC n'a plus ses empreintes digitales, elle non plus.

L'explication qui précède est largement fondée sur une reconstruction des événements basée sur des probabilités. Elle n'a rien de définitif. Le Commissaire a conclu que les renseignements avaient été communiqués à tort, mais, faute de détails, il n'était en mesure de blâmer personne.

Le plaignant est redevenu fonctionnaire fédéral et a récemment fait l'objet d'une vérification périodique de sécurité, pour laquelle la GRC doit consulter son casier judiciaire. Étant donné que personne n'avait retiré la note de distribution figurant sur la vieille liste, le double du casier, mis à jour, a été envoyé à la Société canadienne des postes.

L'enquête a révélé que les Services de sécurité de la Société canadienne des postes avaient reçu de la GRC, au début de 1991, un double du casier judiciaire du plaignant. Bien que ce soit à fait normal quand on fait subir une vérification de sécurité aux employés de la Société ou aux candidats qui y postulent un emploi, rien auprès des Services de sécurité n'indiquait qu'on ait demandé ces renseignements. Le plaignant n'était ni un employé, ni un candidat, et les Services de sécurité avaient rangé le double du casier judiciaire dans un dossier provisoire.

À la demande de l'enquêteur, la GRC a examiné ses dossiers, ce qui lui a permis de trouver la note de distribution « Bureau de poste d'Ottawa » à côté de la mention de la condamnation du plaignant. Toutefois, cela n'explique pas pourquoi la GRC avait envoyé un double du casier judiciaire du plaignant à la Société canadienne des postes.

L'enquête s'est poursuivie et le Commissaire a appris que le plaignant avait travaillé brièvement aux Postes il y a plus de dix ans. À l'époque, il avait fait l'objet d'une vérification de fiabilité (pour laquelle on prend les empreintes digitales); c'est ce qui explique l'existence de la note de distribution au bureau de poste. Une fois que le plaignant a quitté cet emploi, son dossier personnel - avec ses empreintes digitales - aurait normalement dû être transféré au Centre national des dossiers du personnel.

La Société canadienne des postes illustre sa flexibilité sur la question du privilège d'envoi en citant par exemple le cas d'aveugles qui ont déjà retourné des cassettes-phones à l'INCA pour les faire réparer et ce sans payer de frais de poste. L'INCA a déclaré que ce genre d'envoi ne devrait manifestement pas être gratuit.

L'enquêteur a expliqué la procédure et la position de l'INCA au plaignant, qui a dit reconnaître que son droit à l'intimité n'avait pas été violé sans raison par la Société canadienne des postes. Le Commissaire a conclu que la plainte n'était pas bien fondée.

La divulgation était une erreur, mais à qui la faute?

Une plainte portée contre la GRC a montré qu'il est parfois impossible d'arriver au fond du problème.

Un homme s'est plaint au Commissaire quand il a appris que la GRC avait envoyé à la Société canadienne des postes un exemplaire de ses empreintes digitales et de son casier judiciaire, sans qu'on le lui ait demandé. Il n'y avait apparemment aucune raison pour que la GRC divulgue le casier judiciaire du plaignant, étant donné qu'on lui avait accordé un pardon. Autrement dit, son casier aurait dû être scellé.

L'enquêteur du Commissariat a été incapable d'obtenir une explication satisfaisante. La vérification n'a pas donné de résultats probants, et le Commissaire a dû rendre sa décision en se fondant sur le peu d'information dont il disposait.

Le plaignant a accepté que l'enquêteur demande l'avis de l'Institut national canadien pour les aveugles (INCA). L'INCA a expliqué que le privilège d'envoi postal gratuit qui lui est accordé équivaut à une subvention de près de trois millions de dollars par année qu'il ne voudrait pas perdre.

La nature même des cassettes audio fait qu'elles ne peuvent pas être mises à la poste comme des lettres ordinaires; les expéditeurs doivent utiliser des enveloppes cousinées spéciales. Pour les livres «parlants» qui constituent la plus grande partie de ses envois, l'INCA a conçu une pochette de plastique réutilisable, fermée par une bande Velcro, qui est pratique et se prête bien aux inspections. Pour ses autres envois, elle utilise de petites enveloppes cousinées fermées avec du ruban gommé ou des agrafes. La Société canadienne des postes ne s'oppose pas à ce mode de fermeture des enveloppes, et le représentant de l'INCA a déclaré à l'enquêteur n'avoir jamais entendu parler d'un aveugle qui aurait eu des problèmes avec des enveloppes fermées de cette façon.

Selon le représentant de l'INCA, le règlement postal stipule que l'enveloppe doit être fermée de façon que son contenu puisse être facilement inspecté. Il n'est pas interdit de la cacheter. D'après lui, le plaignant n'avait qu'à fermer ses enveloppes avec des agrafes pour qu'il soit relativement facile de vérifier si elles avaient été ouvertes.

Toutefois, l'enquête a révélé que le plaignant demandait chaque année de l'information sur le centre à EIC - en invoquant la Loi à l'accès à l'information -, depuis qu'il s'était querellé avec ses dirigeants. Le personnel du centre le connaissait bien, et il aurait parlé ouvertement de ses demandes d'accès aux dossiers.

Quand la demande est arrivée au Centre, son directeur a tout simplement assumé l'identité du requérant. D'après lui, il ne fallait pas nécessairement être un génie pour cela...

Comme rien ne prouvait qu'EIC avait révélé d'où provenait la demande, le Commissaire a conclu que la plainte n'était pas bien fondée.

Oui, les bandes audio des aveugles peuvent être envoyées sous pli «cacheté»

Un aveugle a porté plainte au Commissaire en disant que la Société canadienne des postes portait atteinte à son droit à l'intimité en exigeant que les aveugles expédient leurs bandes-lettres dans des emballages non cachetés.

L'enquêteur du Commissariat a appris que les aveugles sont autorisés à envoyer leurs bandes-lettres par la poste gratuitement, mais qu'ils doivent les emballer de façon que le personnel de la Société puisse ouvrir facilement l'emballage afin de vérifier si l'envoi est bien conforme aux règlements.

Le délateur anonyme n'était pas EIC

Un plaignant a déclaré au Commissaire qu'Emploi et Immigration Canada avait divulgué à son ex-femme des renseignements sur ses revenus tirés de son dossier d'assurance-chômage. Puis, elle s'était servie de ces renseignements pour s'adresser aux tribunaux afin d'obtenir une augmentation de sa pension alimentaire.

L'enquêteur du Commissariat a interrogé les deux employés d'EIC qui s'étaient occupés du plaignant, et ceux-ci ont nié avoir divulgué des renseignements personnels à son sujet à des personnes qui n'étaient pas été autorisées à les avoir. L'ex-femme du plaignant et son conjoint ont aussi été interrogés; ils ont nié avoir obtenu les renseignements d'EIC, en disant qu'ils leur venaient d'un appel anonyme.

Le Commissaire a conclu que rien ne prouvait l'allégation du plaignant que c'étaient des fonctionnaires d'EIC qui étaient à l'origine de la divulgation et a rejeté la plainte.

Le plaignant a révélé lui-même son identité

Un homme a porté plainte au Commissaire en disant que des représentants d'Emploi et Immigration Canada avaient révélé à un centre subventionné par EIC qu'il avait demandé de l'information à son sujet en vertu de la Loi à l'accès à l'information. Le plaignant a déclaré à juste titre que l'avis identifié à l'organisme en question équivalait à une communication abusive de renseignements personnels.

À la suite de quoi, l'employé s'est plaint au Commissaire à la protection de la vie privée, que Revenu Canada avait divulgué des renseignements personnels sans son autorisation. L'enquête du Commissaire a révélé que des documents personnels avaient été pris et utilisés dans le cadre de l'enquête de harcèlement et que ces renseignements avaient été communiqués à l'extérieur du ministère sans le consentement du plaignant.

Les documents comprenaient l'état de prestations de l'employé — y compris des renseignements médicaux — ainsi que son formulaire de renseignements personnels en entier qui indiquait son niveau de scolarité, les emplois précédents, des références personnelles, de même que les noms des membres de sa famille, les occupations ainsi que les adresses de ces derniers. Le Commissaire a conclu que l'utilisation de ce type de documents personnels au cours d'une enquête interne pouvait difficilement cadrer avec le but de la collecte originale de ceux-ci.

Revenu Canada s'est excusé auprès du plaignant pour avoir communiqué ses renseignements personnels et a modifié son manuel d'enquêtes internes pour s'assurer qu'à l'avenir les enquêteurs n'utilisent ou ne dévoilent pas ce genre de renseignements personnels sans le consentement de la personne.

Au cours d'une enquête à la suite d'une plainte de harcèlement, Revenu Canada (Douanes et accises) fouille le bureau d'un employé soupçonné d'être l'auteur d'une note anonyme laissée sur le bureau d'un collègue. Les enquêteurs de Revenu Canada ont photocopié son annuaire téléphonique et ont prélevé de son dossier personnel des renseignements personnels afin de les soumettre à une analyse par des experts en écriture.

On assomme un maringouin à coups de marteau

La plainte, jugée bien fondée, a donc été résolue.

L'enquête a révélé qu'une copie de la lettre avait effectivement été affichée sur un babillard dans une salle où travaillait le plaignant, et où d'autres employés civils et militaires pouvaient la voir. Il a été établi que le surveillant avait agi sous les ordres de son supérieur dans le but d'informer le personnel de respecter la politique de fumage et anti-tabagisme du ministère. À la suite de l'enquête, les représentants du ministère ont reconnu que la lettre en question n'aurait jamais dû servir de rappel aux employés de ne pas fumer dans les édifices de la Défense nationale. Le ministère a confirmé que des mesures correctives avaient été prises afin d'empêcher qu'une situation semblable ne se reproduise.

Il va sans dire qu'on a besoin de détails sur les antécédents des personnels des fonctionnaires pour faire des vérifications sur ceux qui sont en mesure d'influencer des gens qui ont accès à des secrets mettant en jeu la sécurité nationale. Toutefois, le Commissariat a du mal à comprendre pourquoi le CST a besoin de plus de renseignements personnels sur les antécédents des nouveaux conjoints de ses employés titularisés que sur ceux des conjoints de ses nouveaux employés.

Les dirigeants du CST ont été persuadés d'harmoniser leurs politiques avec celles des autres ministères. Ironiquement, le MDN avait déjà modifié sa politique en ce sens avant que l'enquête ne soit terminée et que le Commissariat le lui demande.

La plainte, jugée bien fondée, a donc été résolue.

Les réponses de grief ne sont pas destinées à un affichage public

Un employé du ministère de la Défense nationale s'est plaint auprès du Commissaire qu'un surveillant avait affiché une copie de la lettre qui lui avait été adressée en réponse à un grief déposé auprès de son employeur. La lettre comportait son nom, son adresse de même que ses idées et ses opinions personnelles relativement à la politique de fumage et anti-tabagisme du ministère.

Toutefois, le CST ne s'est pas arrêté là; il a aussi demandé des détails sur le lieu de résidence et l'emploi de l'intéressée au cours des cinq années précédentes. À ce moment-là, celle-ci a porté plainte au Commissaire à la protection de la vie privée : selon elle, en exigeant ces renseignements supplémentaires, le CST portait atteinte à son droit à l'intimité. De plus, il aurait dû lui demander les renseignements en question directement plutôt que de chercher à les obtenir d'un tiers.

L'enquête a révélé que la politique du CST sur les vérifications de fiabilité est différente de celle de la plupart des autres ministères et organismes fédéraux, qui se contentent des renseignements fournis par les fonctionnaires dans le questionnaire qu'ils remplissent pour obtenir leur autorisation de sécurité. Qui plus est, les fonctionnaires nouvellement embauchés par le CST ne sont pas tenus de fournir ces renseignements détaillés sur leur conjoint. Seuls les fonctionnaires titularisés qui changent de situation familiale doivent fournir des détails sur les antécédents, tels le lieu de résidence et emploi de leur nouveau conjoint.

Le MDN était le seul ministère fédéral à exiger qu'on lui fournisse ces renseignements supplémentaires dans des circonstances analogues. Il demandait des détails sur le lieu de résidence et l'emploi du conjoint au cours des dix années précédentes.

Un fonctionnaire du Centre de sécurité des télécommunications (CST) a informé ses supérieurs qu'il allait se marier, conformément à la procédure que doivent respecter tous les fonctionnaires fédéraux ayant l'autorisation de sécurité «Secret» ou «Très secret». Le fonctionnaire a donc donné le nom, la date de naissance, l'adresse et le nom de l'employeur de sa future épouse, comme l'exige le questionnaire pour l'obtention de l'autorisation de sécurité du gouvernement.

Les nouveaux mariés ont droit à un traitement égal

Les autorités de la CFP ont accepté de traiter de la même façon les demandes d'information fondées sur la Loi qui émanent des plaignants et des intimes, dans les cas où ces derniers sont des particuliers plutôt que des ministères ou organismes. Dans ce cas-ci, tous les renseignements figurant au dossier d'enquête de la CFP seront communiqués au plaignant, sous réserve des autres exceptions prévues par la Loi.

Puisqu'on n'avait pas refusé de communiquer à l'intéressé des renseignements personnels le concernant, sa plainte n'était pas bien fondée. Toutefois, elle a amené la CFP à lui communiquer tout le contenu du dossier qui ne pouvait être protégé par une exception, ainsi qu'à modifier sa méthode de traitement des demandes.

L'intimé devrait avoir accès à tout le dossier

Un plaignant a protesté contre le traitement que la Commission de la Fonction publique (CFP) avait réservé à sa demande de consultation d'un dossier d'enquête sur une affaire de harcèlement. Le Commissariat a constaté que la demande n'avait peut-être pas été traitée de façon conséquente.

Le requérant (qui était l'intimé dans l'affaire de harcèlement) n'avait reçu que les parties du dossier que la CFP considérait comme les renseignements personnels le concernant. L'enquête a révélé que la CFP a différentes façons de traiter les dossiers de harcèlement, en fonction du requérant. Si le requérant est le plaignant, la CFP considère tout le dossier comme un ensemble de renseignements personnels qui le concernent et le lui communique intégralement, hormis les exceptions prévues par la *Loi sur la protection des renseignements personnels*.

Toutefois, si le requérant est quelqu'un d'autre, par exemple un témoin ou l'intimé, la CFP ne lui fournit que les documents qu'elle considère comme des renseignements personnels à son égard.

L'enquêteur du Commissariat s'est dit d'avis que, puisque le requérant était aussi l'accusé de harcèlement, le seul intime, et que tout le dossier avait trait à l'enquête sur une plainte portée contre lui, la CFP aurait dû le lui communiquer intégralement.

Le comité consultatif du CIPC a demandé une opinion juridique sur l'identification des personnes porteuses du VIH et du SIDA, puis il a modifié sa politique, qui interdit maintenant l'identification des personnes porteuses de ces virus à moins qu'un porteur ait menacé de les transmettre en ayant recours à la violence ou qu'il ait été accusé d'avoir enfreint les lois sur la santé publique en transmettant délibérément les virus.

De plus, le CIPC a communiqué avec tous les organismes qui ont accès à ces bases de données pour leur expliquer sa nouvelle politique. Une vérification ultérieure a relevé 96 mentions «C» (les personnes ne sont pas nécessairement porteuses du VIH ou du SIDA). Depuis, le CIPC a envoyé un rappel aux utilisateurs et fait une autre vérification qui a révélé qu'il ne lui restait plus que 40 fiches portant une mention «C», toutes parfaitement justifiées à des fins policières.

Enfin, un représentant de la GRC est allé rencontrer les membres de la coalition à Vancouver, avec l'enquêteur du Commissariat, pour leur expliquer la situation et pour répondre à leurs questions. La coalition a semble satisfait du résultat de l'enquête. Le Commissaire est particulièrement reconnaissant au CIPC et à la GRC de l'ouverture d'esprit avec laquelle les deux organismes ont su écouter les inquiétudes très réelles des organisations intéressées, puis y répondre.

Quelques cas

Le CIPC restreint l'identification des personnes souffrant du SIDA

Un groupe d'organismes communautaires de Vancouver a demandé au Commissaire d'enquêter sur des allégations que les bases de données du Centre d'information de la police canadienne (CIPC) identifiaient les personnes porteuses du VIH qui y figuraient.

Même si personne ne pouvait faire état d'un fait précis et s'il n'est pas du tout sûr que le CIPC relève de sa compétence, le Commissaire a décidé de faire enquête officiellement.

La GRC (qui administre le CIPC) a expliqué que les renseignements sur les individus fichés au Centre pouvaient comporter une mention «C» servant à indiquer que l'intéressé souffre d'une maladie contagieuse. Cette mention a pour objet d'aider la police à trouver les personnes ayant des maladies transmissibles qui se sont évadées ou échappées d'hôpitaux ou de pénitenciers. Elle doit aussi aider la police à prévenir les personnes qui auraient pu être exposées aux maladies véhiculées par ces porteurs.

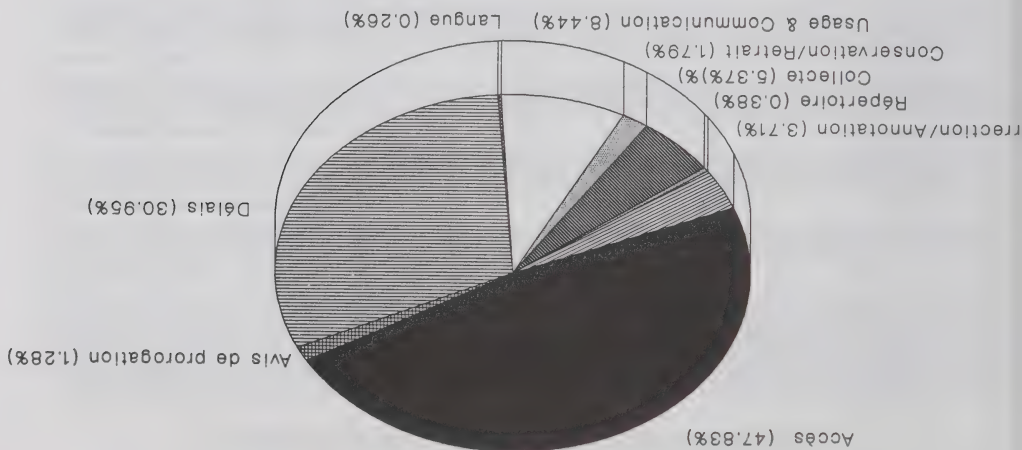
Plaintes réglées par institutions et résultats

Résultats					Ministère	
NOMBRE	Bien fondée	Bien fondée; résolue	Non fondée	Abandonnée		
110	25	10	65	10	Défense nationale	
71	11	22	30	8	Emploi et Immigration Canada	
1	0	0	1	0	Forêts Canada	
44	0	1	40	3	Gendarmerie royale du Canada	
8	0	1	7	0	Justice Canada	
1	0	0	1	0	Monnaie royale canadienne	
10	1	1	8	0	Pêches et Océans	
25	15	4	5	1	Revenu Canada, Douanes et Accise	
67	31	4	31	1	Revenu Canada, Impôt	
7	2	0	5	0	Santé et Bien-être social Canada	
2	0	0	1	1	Secrétariat d'Etat du Canada	
56	0	5	42	9	Service canadien du renseignement de sécurité	
130	10	25	76	19	Service correctionnel Canada	
67	2	9	55	1	Société canadienne des Postes	
1	0	1	0	0	Société du crédit agricole Canada	
5	0	0	5	0	Solliciteur général Canada	
3	0	0	1	2	Statistique Canada	
20	2	12	6	0	Transports Canada	
3	2	0	1	0	Travail Canada	
2	0	0	2	0	Travaux publics Canada	
782	152	117	448	65	TOTAL	

Plaintes réglées par institutions et résultats

Ministère				Résultats	
NOMBRE	Bien fondée	Bien fondée; résolue	Non fondée	Abandonnée	
Anciens combattants Canada	7	0	0	7	0
Affaires extérieures Canada	13	0	7	6	0
Affaires indiennes et du Nord Canada	11	7	0	4	0
Agriculture Canada	3	0	2	1	0
Approvisionnement et Services Canada	7	1	0	6	0
Archives nationales du Canada	10	2	1	6	1
Banque du Canada	2	0	1	1	0
Bureau du Conseil privé	1	0	0	1	0
Bureau de surintendant des institutions financières Canada	3	2	1	0	0
Commissariat aux langues officielles	1	0	1	0	0
Commission canadienne des droits de la personne	2	0	0	2	0
Commission de contrôle de l'énergie atomique	1	0	1	0	0
Commission de l'immigration et du statut de réfugié	34	33	0	0	1
Commission de la Capitale nationale	1	0	0	1	0
Commission des relations de travail dans la Fonction publique	1	0	0	1	0
Commission nationale des libérations conditionnelles	35	6	5	23	1
Communications	1	0	0	1	0
Conseil de la radiodiffusion et des télécommunications canadiennes	1	0	0	1	0
Consommation et Corporations Canada	9	0	0	3	6

Plaintes réglées par motifs 1991-92



Origine des plaintes réglées

5	Terre-Neuve
4	Prince-Édouard
43	Nouvelle-Écosse
20	Nouveau-Brunswick
48	Québec
17	Région de la Capitale nationale - Québec
114	Région de la Capitale nationale - Ontario
226	Ontario
28	Manitoba
30	Saskatchewan
94	Alberta
144	Colombie-Britannique
4	Territoires du Nord-Ouest
2	Yukon
3	For Canada
782	TOTAL

L'examen de ces deux fichiers par le personnel du Commissariat a démontré qu'ils sont constitués principalement de renseignements personnels préparés ou obtenus dans le cadre d'enquêtes criminelles, dont la divulgation risquerait vraisemblablement de porter préjudice à la conduite des affaires internationales du Canada ou à sa défense (articles 21 et 22 de la Loi sur la protection des renseignements personnels). Le Commissaire ne désire pas se prononcer sur la validité de ces dispenses afin d'éviter de se placer en situation de conflit d'intérêt au cas où il recevrait une plainte sur des renseignements conservés dans ces fichiers.

Demande pour plus de ressources

Avec une augmentation de 13 pourcent dans le nombre des plaintes reçues au cours de l'exercice, le Commissariat se retrouve avec un arriéré qui correspond à presque une année de travail — 1 209 plaintes en souffrance à la fin de l'année. Comme nous l'avions annoncé dans le rapport annuel de l'an dernier, ceci a eu pour effet d'augmenter la charge de travail des enquêteurs à 200 chacun. En conséquence, les clients doivent maintenant s'attendre à des délais plus longs afin d'obtenir la décision du Commissaire sur leurs plaintes.

Le Conseil du Trésor a alloué au Commissariat deux années-personnes additionnelles afin d'augmenter le nombre d'agents à la vie privée. Mais si les plaintes continuent d'arriver au même rythme que l'an passée, le Commissariat se retrouvera avec plus de 2 000 dossiers d'enquêtes ouverts. Une telle situation risque de devenir incontrôlable.

Propositions pour de nouveaux fichiers inconsultables

Le Commissariat a été consulté à deux reprises au cours de l'année sur des propositions visant l'établissement de deux nouveaux fichiers inconsultables. La GRC a avisé le Commissaire de son intention de demander l'approbation du Cabinet afin de créer un fichier inconsultable pour ses dossiers d'enquêtes relatives à la sécurité nationale. Le SCRS a également informé le Commissaire relativement à son projet de présenter une demande pour la création d'un fichier inconsultable touchant ses dossiers d'enquêtes.

TOTAL		1,402		651		467		284	
AUTRE		273		119		55		99	
Archives nationales du Canada		47		14		23		10	
Commission de l'immigration et du statut de réfugié		68		33		33		2	
Revenu Canada, Douanes et Accise		72		29		31		12	
Gendarmerie royale du Canada		84		67		4		13	
Service canadien du renseignement de sécurité		87		77		10		0	
Défense nationale		99		20		63		16	
Revenu Canada, Impôt		107		27		59		21	
Emploi et Immigration Canada		135		72		26		37	
Société canadienne des Postes		143		101		3		39	
Service correctionnel du Canada		287		92		160		35	
Ministère		NOMBRE		Accès		Détails		Autre	
								Moins	

Les dix ministères les plus visés selon les plaintes reçues

La GRC continue de se distinguer par le maintien du très grand respect qu'elle accorde pour l'esprit et la lettre de la Loi. Seulement une des plaintes portées contre elle s'est révélée bien fondée, tandis que 40 n'étaient pas fondées et que trois autres ont été abandonnées. Le SCRS doit aussi être félicité : sur les 56 plaintes portées à son endroit, seulement cinq ont été trouvées bien fondées, et elles ont toutes été résolues.

L'an passé le SCC a eu la plus haute proportion de plaintes bien fondées, avec Emploi et Immigration Canada, Revenu Canada (impôt) et la Défense nationale qui n'étaient pas très loin derrière. Cette année, même s'il continue d'être au premier rang pour le nombre de plaintes reçues (un total de 287), seulement 27 pourcent des plaintes portées à son endroit, se sont avérées bien fondées. Environ la moitié des plaintes portées contre Emploi et Immigration Canada et Revenu Canada (impôt) et 32 pourcent de celles à l'endroit de la Défense nationale ont été considérées bien fondées.

Le nombre de plaintes abandonnées cette année est élevé. Il se chiffre à 65, ce qui représente 8 pourcent des dossiers qui ont été fermés. Cependant, la majorité ont été abandonnées lorsque les institutions gouvernementales ont été avisé de notre intention d'enquêter, ce qui les à inciter à résoudre le problème. Évidemment, c'est ce en quoi consiste le rôle d'un ombudsman—résoudre des problèmes, non compter des plaintes.

Vers la fin de l'année fiscale, le bureau a modifié sa façon de comptabiliser les plaintes de délais. Fréquemment, les plaignants remettaient en question les avis de prorogation du délai de 30 jours expédiés par les ministères lorsque ceux-ci voulaient consulter d'autres organisations ou lorsque l'observation du délai entraverait de façon sérieuse le fonctionnement de l'institution. Notre bureau ne comptabilisait pas le nombre de plaintes qui visaient les avis de prorogation du délai. Les plaintes de délais sont maintenant divisées en deux catégories : le non respect du délai et l'avis de prorogation du délai. Cela contribue aussi à identifier les ministères qui continuent de négliger de répondre aux demandes en temps.

Dans des périodes de restrictions budgétaires, il est difficile de prêcher aux ministères la nécessité de respecter les délais. Les budgets et le personnel ont été diminués dans la plupart des ministères et le service au public en souffre.

Quoique le nombre de plaintes de délais et d'accès reçues ont augmenté de 31 pourcent, de 855 l'an passé à 1 118 en 1991-1992—le nombre de plaintes concernant les collectes, les usages et les communications non autorisés de renseignements personnels a chuté de 26 pourcent—de 384 en 1990-1991 à 284 en 1991-1992.

Le rapport de l'an dernier applaudissait les efforts du Service correctionnel du Canada pour circonscrire son problème de non respect des délais. Malheureusement, les plaintes de délais ont triplées cette année—160 (comparé à 50 l'an passé). Ces plaintes représentent 34 pourcent de notre volume de plaintes de non respect des délais. Cependant, ceci nécessite une explication. Le SCC a modifié ses procédures de traitement des renseignements des détenus qu'il reçoit des gouvernements municipaux et provinciaux ainsi que des services de police. Le SCC effectuait auparavant automatiquement des dispenses à l'information confidentielle reçues des autres gouvernements. Cependant, après quelques années de pression exercée par notre bureau, le SCC demande maintenant aux organismes d'où proviennent les informations, la permission de les communiquer.

Ceci occasionne des délais pour les demandeurs. Face à l'augmentation de sa charge de travail et la diminution de ses ressources, le SCC doit choisir le moindre mal : donner une réponse incomplète mais en respectant les délais—ou donner des réponses plus satisfaisantes, mais risquer de dépasser les délais prescrits.

D'autres ministères ont aussi de la difficulté à rencontrer les délais : les Archives nationales, Revenu Canada (impôt) et la Défense nationale.

Une autre hausse importante est survenue à Revenu Canada (Douane et accises). Leurs 72 plaintes représentent une augmentation cinq fois supérieure aux données de l'an passé.

TOTAL		152	117	448	65	782
	Avis de prorogation	4	0	6	0	10
	Délais	138	3	90	11	242
Délais		142	3	96	11	252
	Usage & Communication	3	9	51	3	66
	Conservation/Retrait	1	1	6	6	14
	Collection	1	2	35	4	42
Atteinte à vie privée		5	12	92	13	122
	Langue	0	2	0	0	2
	Répertoire	0	0	3	0	3
	Correction/Annotation	0	0	29	0	29
	Accès	5	100	228	41	374
Accès		5	102	260	41	408
Motifs		Bien fondée	Bien fondée: résolue	Non fondée	Abandonnée	NOMBRE
Résultats						

Plaintes par motifs et résultats

S'est joint à la liste, la Commission de l'immigration et du statut de réfugié (CISR) avec 68 plaintes — les premières plaintes concernant la vie privée reçues à l'endroit du CISR. Cependant, 67 de ces plaintes furent déposées par le même plaignant, incluant 33 plaintes de délais considérées bien fondées. Les enquêtes concernant les 33 plaintes d'accès sont en cours.

Notre bureau a fait part de ses préoccupations face à l'administration du CIPC dans des rapports antérieurs et a recommandé que la GRC consulte les utilisateurs du CIPC afin qu'on introduise un Code de protection volontaire des renseignements personnels dans les bases de données. Ceci contribuerait à instaurer une meilleure protection en ce qui concerne la collecte, l'usage et la communication des renseignements personnels, et permettrait aux individus d'avoir accès à leurs renseignements personnels et de corriger ces informations, s'il y a lieu.

Des félicitations s'imposent. En effet, le CIPC a approuvé et mis en oeuvre un code d'éthique en novembre 1991, code qui rejoint nos préoccupations—particulièrement celles touchant les droits d'accès. Il permet aux individus de demander accès à leurs renseignements personnels contenus dans le CIPC et de demander une correction, lorsque nécessaire.

Les dix premiers

L'an passé, pour la première fois le Commissariat identifiait ses dix plus gros clients—un groupe qui représentait 80 pourcent du total de sa charge de travail. Huit de ces dix ministères font de nouveau la liste cette année : le Service correctionnel du Canada, la Société canadienne des postes, Emploi et Immigration Canada, Revenu Canada (Impôt), la Défense nationale, le Bureau canadien du renseignement de sécurité, la GRC et les Archives nationales.

C'est la première fois que notre Bureau entreprend une enquête aussi longue et complexe et cela nous a coûté beaucoup. Les presque six mois qu'y ont consacré trois enquêteurs principaux, ont fait qu'ils n'ont pu se vouer à d'autres tâches. C'est la raison principale qui explique qu'il y ait moins de dossiers complétés que l'an passé. Le roulement dans le personnel (et la formation des nouveaux venus) y ont aussi contribué, augmentant la pile de dossiers non réglés.

Une nouvelle politique au sujet de CIPC

Le Centre d'information de la police canadienne (CIPC) continue d'être la cible de plaintes et de demandes de renseignements concernant la cueillette, l'usage et la communication des renseignements personnels que sa base de données renferme. Le CIPC, constitué de bases de données policières est subventionné par le fédéral et administré par la GRC. Cependant, il est chapeauté par un Comité consultatif constitué des principaux services de polices municipaux et provinciaux, qui contribuent et ont accès aux renseignements.

Plusieurs nous disent qu'ils ne peuvent obtenir leurs renseignements personnels sur le CIPC parce que les services de police ne peuvent pas divulguer des renseignements qui leur ont été fournis par d'autres. Par exemple, la GRC ne peut communiquer des renseignements reçus du service de police d'Ottawa.

Le Bureau a reçu 1 402 nouvelles plaintes cette année en comparaison de 1 239 l'an dernier—une augmentation de 13 pourcent. Cette augmentation suit le même scénario que celui établi par le bureau depuis sa création en 1983. Ce qui diffère est la diminution du nombre de dossiers complétés. Les enquêteurs ont fermés 782 cas, dont 269 étaient bien fondés, 448 étaient non bien fondés et 65 ont été abandonnés.

Le recensement de 1991

Au cours de la dernière année, ce dossier a retenu beaucoup de notre attention; nous avons enquêté sur 34 plaintes au sujet du recensement de 1991. Plusieurs plaignants étaient préoccupés par la collecte de renseignements personnels effectuée par Statistique Canada et ont refusé de répondre aux questions du recensement, celles-ci leur paraissant manqué de respect envers leur vie privée.

D'autres ont fait valoir la promesse (ou l'absence) de confidentialité entourant les réponses au recensement. La plainte la plus fréquente à ce sujet était que des voisins ou des connaissances, employés lors du recensement, en recueillaient les résultats. Les plaignants croyaient que leur questionnaire complété serait envoyé directement à Statistique Canada à Ottawa et qu'il serait révisé par un fonctionnaire anonyme, et non par quelqu'un de leur quartier. L'enquête tire maintenant à sa fin et ses résultats seront partagés avec Statistique Canada.

Un complément d'information s'impose : le Commissariat a été enfin avisé de l'intention d'Agriculture Canada de coupler les données des dossiers du Bureau d'examen de l'endettement agricole avec ceux du ministère de l'Agriculture du Québec, afin de faciliter le fonctionnement d'un nouveau programme de subvention des exploitants de parcs d'engraissement de bovins et de médiation avec les créanciers des agriculteurs. Toutefois, le Commissariat n'a pas reçu assez de détails pour évaluer ce couplage.

Couplages de données agricoles

En toute justice, il faut reconnaître qu'Agriculture Canada a scrupuleusement respecté la politique sur le couplage de données. Dans le premier avis il l'a informé que la nouvelle *Loi sur la protection du revenu agricole* l'autoriserait à coupler les données sur les agriculteurs tirées du compte de stabilisation du revenu avec les données sur les revenus de Revenu Canada.

Grâce à ce couplage, les prestations versées aux agriculteurs par ce programme seront calculées en fonction de renseignements exacts sur leurs revenus, leurs dépenses et leur production. La Loi donne à Agriculture Canada le pouvoir légal de faire les couplages nécessaires, en l'autorisant à utiliser le numéro d'assurance sociale des intéressés.

Saisies pour besoins familiaux : Agriculture Canada a aussi avisé le Commissaire de son intention de coupler les données tirées du Programme de stabilisation concernant le grain de l'Ouest avec celles du ministère de la Justice, pour qu'il soit possible de saisir les paiements versés par ce programme aux agriculteurs qui ne paient pas leurs pensions alimentaires et autres types de contributions aux besoins de leur famille. En réalité, il n'était pas nécessaire que le ministère soumette sa proposition au Commissariat, puisque le Parlement a pris un règlement, en vertu de la *Loi d'aide à l'exécution des ordonnances et des ententes familiales*, afin d'autoriser des retenues à même le Programme de stabilisation.

genre au moins 60 jours à l'avance. Le Commissaire évalue alors la validité du couplage en fonction d'une série de critères et se fait le défenseur de ceux qui font l'objet des dossiers visés. Il s'agit en somme d'empêcher le gouvernement d'entreindre, par souci d'efficacité, les droits des gens à la protection des renseignements personnels les concernant.

C'est une politique admirable, mais peut-être pas très efficace. Seulement 22 organismes fédéraux ont dans le répertoire des renseignements fédéraux, *Info Source*, des inscriptions décrivant quelque chose qui ressemble - même de loin - à un couplage de données. Il est bien connu que certains ministères rangent les couplages sous des rubriques plus anodines "d'utilisation" ou de "divulgateur". D'autres organismes ne reconnaissent l'existence d'un couplage que lorsqu'il y a une liaison entre leurs données et celles d'un organisme distinct, ce qui est contraire à la politique qui s'applique clairement aussi au couplage de fichiers de différents programmes d'un même organisme.

Tout ce que le Commissaire a vu jusqu'à présent l'amène à conclure que le couplage de données informatiques est un phénomène courant au gouvernement, particulièrement dans le cas des programmes sociaux, des activités d'application de la loi et de recherche de renseignements et du système de justice pénale. Les fonctionnaires sont-ils capables d'identifier les couplages de données? Sont-ils au courant de la politique? La considèrent-ils simplement comme un obstacle à contourner?

Bref, le Commissaire presse le Conseil du Trésor d'enquêter. Cela dit, ses équipes de vérification de l'observation ont ajouté le couplage de données à leur liste de critères de vérification.

Il semble bien que l'expérience ait été couronnée de succès et le nouveau code sera utilisé dans le programme national. EIC donnera ce numéro code aux prestataires pour qu'ils puissent s'identifier lorsqu'ils feront des demandes de renseignements par téléphone. Les prestataires pourront aussi choisir leur propre numéro de code, s'ils le désirent.

Le Commissaire applaudit à la rapidité de réaction d'EIC et à sa sensibilité à protéger sa clientèle.

Couplage de données

Dans ce domaine, la meilleure nouvelle de l'année, c'est qu'on a signalé au Commissariat très peu de nouveaux cas de couplage de données. Le Commissaire n'a reçu que trois avis au cours de l'année écoulée, tous provenant d'Agriculture Canada.

Le Commissaire ne voudrait pas sembler trop soupçonneux. Néanmoins, il serait vraiment crédible s'il souscrivait à l'idée qu'un seul organisme fédéral sur plus de 150 qui sont soumis à la politique de couplage des données du gouvernement aurait commencé en 1991-1992 à coupler des dossiers distincts.

La politique de couplage interdit de relier des bases de données informatiques susceptibles de produire des dossiers détaillés (appelés «superdossiers») sur les particuliers. Les organismes fédéraux doivent aussi soumettre au Commissaire leurs propositions de ce

Néanmoins, les concepteurs de systèmes d'EIC se sont montrés sensibles aux inquiétudes du Commissariat. Ils ont profité du projet pilote de Peterborough pour tester un nouveau code téléphonique d'accès à quatre chiffres semblable à un numéro bancaire.

Le Système permettait aux usagers du téléphone à clavier de communiquer par téléphone avec un ordinateur pour obtenir de l'information d'ordre général sur leurs demandes de prestations d'assurance-chômage. Par exemple, ils pouvaient confirmer si leur demande avait été acceptée et quand ils commenceraient à toucher leurs prestations. Les intéressés s'identifiaient en donnant leur numéro d'assurance sociale (NAS) et leur date de naissance. Le Commissariat avait été informé de l'existence du système par une station de radio locale, qui lui avait demandé si cette utilisation du NAS était autorisée. Il est certain qu'EIC peut se servir du NAS pour identifier les prestataires de l'assurance-chômage : le NAS a été conçu expressément à cette fin. Cependant, le Commissaire s'inquiétait du manque de protection de la combinaison NAS-date de naissance. Le Commissariat a discuté du problème avec les représentants d'EIC, qui ont reconnu que ces deux types de renseignements personnels sont très répandus, de sorte qu'ils ne constituent pas un code d'accès très bien protégé. Malheureusement, le projet pilote avait déjà gagné London et Peterborough et il semblait trop tard pour le modifier.

Le groupe chargé des applications, qui a pour objectif ultime d'établir des normes et des lignes directrices pour toutes les applications futures des cartes à mémoire dans l'administration fédérale, définira comment les institutions gouvernementales pourraient utiliser ces cartes et dans quel contexte elles devraient être employées. Les membres de ce groupe comptent des représentants d'organismes fédéraux comme Santé et Bien-être social Canada, Approvisionnements et services Canada, la GRC et Anciens combattants Canada, de même que des ministères de la Santé du Québec et de l'Ontario.

Le Commissariat est aussi représenté au groupe d'intérêts spéciaux chargé des normes sur la téléconsultation de systèmes informatiques. Étant donné que de nombreux organismes gouvernementaux ont des intérêts communs en matière d'accès, ils partagent les frais de recherche et de développement et contribuent à l'établissement de ces normes communes.

Le projet SRVA

Dans le rapport annuel de l'an dernier, (page 63), le Commissaire avait décrit une des lacunes du projet pilote de Système de réponse vocale automatisée qu'Emploi et Immigration Canada (EIC) avait amorcé à Québec. Ce passage du rapport se terminait sur une mauvaise note, puisque le projet semblait trop avancé pour être modifié. Toutefois, EIC a rédigé une nouvelle conclusion et le Commissaire en est plus que ravi.

Si nous voulons éviter cela, nous devons d'abord commencer par assurer la transparence des systèmes pour les clients. Les porteurs de carte doivent connaître leurs droits intrinsèques quand ils se servent de leur carte; ils doivent aussi savoir quels renseignements la carte contient, comment elle sera utilisée et quels sont les risques.

Les gens devraient avoir le droit de refuser la carte sans risquer de limiter leur accès aux services. De même, les détenteurs de carte ne devraient pas être avantagés par rapport à ceux qui refusent d'en avoir une.

Enfin, les systèmes et leurs participants doivent respecter à la fois la législation sur la protection de la vie privée et les principes d'éthique fondamentaux régissant la collecte, le traitement et la divulgation des renseignements personnels.

Les risques de sécurité inhérents aux projets pilotes inquiétaient tellement le Commissaire que son personnel a été invité à participer à deux groupes de travail du gouvernement fédéral, l'un chargé d'étudier les applications de la nouvelle technologie et l'autre responsable de l'établissement de normes de téléconsultation des systèmes informatiques.

La carte à mémoire ressemble à une carte bancaire ou à une carte de crédit, mais avec une différence fondamentale. Ces cartes sont porteuses d'une puce de circuits intégrés qui leur donne la capacité de traiter des données et d'en emmagasiner. Grâce aux puces et à la présentation numérique des renseignements, les cartes peuvent aussi contenir une photographie invisible du porteur, voire ses empreintes digitales. Elles pourraient être utilisées pour fournir des services bancaires, téléphoniques et médicaux et pour donner à leurs utilisateurs l'accès à tout un réseau d'ordinateurs.

Besoins de protection de la vie privée

De toute évidence, les cartes à mémoire représentent un important progrès technique susceptible d'améliorer le service à la clientèle des ministères et organismes gouvernementaux et de les aider à limiter leurs frais. C'est particulièrement vrai dans le cas d'organismes comme l'EC, qui doivent suivre une clientèle assez nombreuse, créditer des déductions et verser des prestations.

Néanmoins, les organismes gouvernementaux et leurs clients devraient pouvoir jouir des avantages du progrès sans sacrifier pour autant le contrôle de l'individu sur les renseignements personnels qui le concernent. En fait, les cartes à mémoire pourraient bien devenir la carte d'identité universelle à laquelle les Nord-Américains résistent si farouchement. Leur invention risque de transformer radicalement la relation entre l'individu et l'Etat.

Derniers progrès technologiques

L'an dernier, le Commissaire faisait état dans son rapport des projets d'emploi et Immigration Canada (EIC) de mettre à profit les dernières découvertes informatiques pour mieux servir son énorme clientèle. EIC avait lancé deux projets pilotes, l'un faisant appel à des cartes à mémoire et l'autre à un Système de réponse vocale automatisée (SRVA).

EIC n'est pas le seul organisme fédéral qui ait songé à l'informatique pour améliorer son service. Anciens combattants Canada a déjà fait des essais avec des cartes à mémoire dans le but d'améliorer ses systèmes d'envoi et de facturation de médicaments sur ordonnance aux anciens combattants. En outre, Revenu Canada étudie la possibilité de faire utiliser ces cartes par les voyageurs pour déclarer des marchandises ou payer des droits aux postes de douane.

Plusieurs ministères collaborent actuellement en vue de mettre au point des cartes à mémoire rendant possible la téléconsultation des ordinateurs gouvernementaux. Cela permettrait aux gens qui ont un ordinateur personnel chez eux de communiquer par téléphone avec les ordinateurs des organismes gouvernementaux. Bien entendu, à l'instar de bien d'autres applications de la technologie moderne des communications, ces projets ont des implications pour la vie privée.

Le Commissariat a été saisi de ce qui semble être une utilisation abusive du NAS à la nouvelle banque automatisée de renseignements sur les emplois d'Emploi et Immigration à St. John's (Terre-Neuve). Il s'agit d'un projet pilote grâce auquel les personnes qui recherchent un emploi peuvent consulter une liste informatique des postes disponibles afin de choisir ceux qui correspondent à leurs intérêts et à leurs aptitudes. Le système offre des possibilités accrues au public et libère du personnel d'EIC, qui peut alors vaquer à d'autres tâches.

Toutefois, quelqu'un s'est plaint en disant qu'il n'avait même pas pu voir la liste sans donner son NAS. Selon le plaignant, vu que n'importe quel passant peut consulter sur papier les offres d'emploi disponibles, exiger la production d'un NAS pour donner accès à une liste informatique était exagéré et même inutile, puisqu'il ne réclamait pas de prestations d'assurance-chômage. Il semble qu'EIC ait demandé le NAS pour mesurer à la fois l'efficacité de son système et sa capacité de placer des prestataires de l'assurance-chômage. Quand le Commissariat le lui a demandé, EIC a reconnu que son système devrait être également accessible aux gens qui ne touchent pas de prestations d'assurance-chômage.

Depuis, le système a été modifié. Au départ l'écran affiché informe les utilisateurs que l'accès au système est libre. Les prestataires de l'assurance-chômage ont le choix d'y introduire leur NAS, de façon que le Centre d'emploi du Canada ait une indication de leur recherche d'emploi. Le changement sera incorporé dans le nouveau système national de banque d'emplois.

Que celui qui est sans péché lance la première pierre : renumération de la Fonction publique

La politique de l'administration fédérale de réduire son utilisation du NAS a d'importantes conséquences; ainsi il lui faut renumérer quelque 310 000 fonctionnaires, militaires et membres de la GRC.

Approvisionnement et Services Canada, (responsable des bases de données de la rémunération et des dossiers), commencera en janvier 1993 à attribuer un nouveau code d'identification de dossier personnel (NIP). Chaque membre de la Fonction publique se verra attribuer deux numéros, un NIP et un autre numéro qu'il pourra divulguer à des tiers, par exemple à ses institutions bancaires, compagnies d'assurance et syndicats. Ce deuxième numéro garantira la confidentialité du NIP, tout en permettant à l'employeur de relier à l'intéressé les opérations que celui-ci a faites avec des tiers.

Les gens ne sont pas encore tout à fait sûrs quand une demande de divulgation du NAS est justifiée. Par exemple, les responsables des programmes d'examen des connaissances linguistiques de la Commission de la Fonction publique demandent encore leur NAS aux fonctionnaires, et les syndicats de la Fonction publique continuent eux aussi à s'en servir pour leurs listes de membres. Ces demandes-là sont justifiées. Néanmoins, une fois la renumération des postes menée à bien, le Commissaire recommandera aux fonctionnaires et autres membres de l'administration fédérale de ne pas divulguer leur nouveau NIP.

L'affaire intéresse le Commissariat, même si elle est bien loin de la *Loi sur la protection des renseignements personnels*. Néanmoins, elle soulève une importante question pour la protection de la vie privée : quel programme ou quelle activité d'Emploi et Immigration Canada (ministère responsable de l'attribution du NAS) autorise à attribuer ce numéro à des nouveau-nés?

Le NAS a été créé aux fins de l'assurance-chômage et du Régime de pensions du Canada; par la suite, Revenu Canada a été autorisé à l'utiliser pour les déclarations d'impôt sur le revenu des particuliers. Ces dernières années, le gouvernement fédéral a adopté une politique - louangée par le Commissaire - qui a mis fin à de nombreuses utilisations abusives du NAS dans l'administration fédérale. Toutefois, pour attribuer un NAS aux nouveau-nés, il semble qu'EIC se fonde toujours sur une entente fédérale-provinciale conclue en 1970, soit bien avant que le gouvernement n'ait pris des mesures pour protéger la vie privée.

Le Commissaire a demandé à Emploi et Immigration de lui dire s'il existe une relation directe entre ses programmes et le fait qu'il assigne un NAS aux fins de l'enregistrement des naissances. S'il n'y a pas de relation de ce genre, il compte presser EIC de repenser son entente avec les autorités provinciales de l'île-du-Prince-Édouard, prenant en considération à la fois la *Loi sur la protection des renseignements personnels* et la politique actuelle du gouvernement fédéral, qui limite l'utilisation du NAS à une courte liste de programmes sociaux.

Née sans NAS

La résistance aux demandes de divulgation du numéro d'assurance sociale (NAS) a pris une tournure inhabituelle cette année, quand un couple de l'Île-du-Prince-Édouard a refusé de demander un NAS pour son bébé.

Le service des statistiques vitales de la province exige que tous les nouveau-nés se fassent attribuer un NAS, utilisé comme numéro d'identité pour le Régime provincial de paiement des services de santé. Le couple a demandé une exemption qui lui a été refusée, et le ministère provincial de la Santé a réagi en refusant d'honorer toutes les demandes de remboursement de frais médicaux de leur enfant, parce que celle-ci n'avait pas de NAS.

Le couple a traîné l'affaire devant les tribunaux, en alléguant qu'obliger le bébé à avoir un NAS (et rejeter leurs demandes de remboursement de frais médicaux) viole plusieurs dispositions de la *Charte canadienne des droits et libertés*. Selon les parents, l'enfant n'a aucune obligation légale d'obtenir un NAS avant de commencer à occuper un emploi assurable. En outre, en rejetant les demandes de remboursement de frais médicaux, les autorités provinciales ont contrevenu aux dispositions de la *Charte* sur la protection contre les fouilles et saisies abusives et elles ont refusé au bébé le droit à l'égalité devant la loi; de plus, obliger un bébé à avoir un NAS porte atteinte au droit de chacun à une protection raisonnable de sa vie privée.

Le Commissariat et le ministère des Communications étudient actuellement toute la question de l'impact des télécommunications sur la vie privée et se penchent sur les solutions possibles.

Nouvelle Loi sur les télécommunications

Le projet de *Loi sur les télécommunications* pourrait être un pas dans la bonne direction, puisque le Parlement y reconnaît les dangers de la technologie des télécommunications pour la vie privée. La Loi a notamment pour objectif

“...satisfaire les exigences économiques et sociales - notamment quant à la protection de leur vie privée - des usagers des services de télécommunication...”

De plus, la Loi autorise le gouvernement et le CRTC à interdire les intrusions comme les appels téléphoniques et les messages télécopiés indésirés dans la vie privée des citoyens.

Le Commissariat a l'intention de suivre l'évolution de ce projet de loi à la Chambre, pour s'assurer que les mesures de protection de la vie privée ne sont pas touchées. Et l'on se demande si les dispositions prises vont assez loin. La Loi ou ses règlements devraient mettre en évidence les normes qui s'appliquent à la vie privée que les services de télécommunications devraient rencontrer.

Bref, le débat a focalisé l'attention du public sur la protection de la vie privée. Néanmoins, ce qui est sans doute plus inquiétant, c'est le fait qu'on sait bien que ces services ne sont qu'un début, l'un des premiers éléments d'un système intelligent de réseaux en expansion croissante. Ce système offrira bientôt des réseaux de communication personnels où les usagers auront un numéro de téléphone personnel leur vie durant, des services de composition et des téléphones à écran. La technologie évolue si vite que ni les ingénieurs, ni les décideurs n'ont le temps de réfléchir à ses impacts sociaux. Chaque nouvelle découverte sape ou perce les barrières érigées si laborieusement contre la précédente pour protéger notre vie privée.

De toute évidence, les maigres ressources du Commissariat à la protection de la vie privée ne lui permettent pas de se maintenir au diapason de chaque nouvelle merveille technique; il n'a ni les compétences, ni l'effectif nécessaire. Néanmoins, le Commissaire tient à trouver des solutions pratiques durables.

L'approche adoptée par l'État de New York présente beaucoup d'intérêt. En effet, la Commission des services publics de l'État s'est donné huit principes généraux de protection de la vie privée dans le domaine des télécommunications. Ceux-ci précisent que les compagnies de télécommunications devraient reconnaître explicitement le droit à la vie privée de leurs clients, de sorte que ceux-ci ne devraient pas avoir à payer davantage pour maintenir la protection dont ils bénéficient actuellement. Les clients devraient être informés de toute utilisation qu'on se propose de faire des renseignements qui les concernent et ils devraient y consentir, s'ils le désirent, en toute connaissance de cause.

Cela dit, le Canada n'est pas le seul pays à s'efforcer de trouver des solutions appropriées aux problèmes causés par le progrès technologique. Aux États-Unis, le débat fait rage depuis que le New Jersey a introduit un service analogue en 1987, et l'on compte parmi les intervenants des commissions de services publics, des législatures d'État, la législature fédérale et même les tribunaux.

Les solutions vont d'un extrême à l'autre. Au New Jersey, on n'offre aucun service de blocage. En Pennsylvanie, l'État a jugé le SGA illégal, puisqu'il contrevient à sa loi sur l'écoute électronique.

Au Texas, on voudrait que l'utilisateur paye pour avoir l'affichage et dans un cas récent, un juge siégeant dans une affaire de droit administratif en Californie a proposé que la Commission des services publics de l'État interdise l'affichage du numéro de téléphone du correspondant qui appelle, parce que cet affichage n'est pas d'intérêt public et viole à la fois les dispositions de l'État et du gouvernement fédéral sur le droit à l'intimité garanti par la Constitution.

D'autres États offrent le blocage de l'affichage gratuit par appel, une facturation par ligne ou encore le blocage de l'affichage gratuit par appel **et** par ligne. Quand le débat battait son plein, une compagnie de téléphone a même offert un service permettant aux usagers de refuser automatiquement les appels bloqués. Les possibilités sont légion.

Bref, toutes ces craintes sont fondées, et les solutions pratiques sont difficiles à trouver. Le SGA peut varier selon la compagnie de téléphone, de sorte qu'on aboutit avec une kyrielle de mesures de protection disparates. Certaines compagnies autorisent les correspondants qui appellent à bloquer l'affichage du numéro pour tous les appels faits sur leur ligne (ou seulement pour certains appels), mais elles leur font payer ce service. Certaines autres ne facturent rien pour bloquer l'affichage. D'autres encore offrent une sorte d'encryptage qui brouille le numéro. De plus, presque toutes les compagnies ont une solution particulière à l'intention des refuges pour femmes.

La plus récente décision rendue à l'égard du SGA émane du Manitoba Public Utilities Board, qui a approuvé la demande de projet pilote de Manitoba Telephone Services à condition que tous les abonnés de la compagnie aient droit à un service gratuit de blocage des appels. Les autorités manitobaines ont aussi exigé un blocage gratuit de la ligne pour les refuges et pour les victimes de violence. Toutefois, elles n'ont pas approuvé le service de retour d'appel, qui conserve les numéros des correspondants ayant fait des appels restés sans réponse pour les afficher plus tard sur commande.

Fait important, le CRTC a récemment annoncé bien après la fin de notre exercice, que les entreprises de téléphone sous sa juridiction doivent offrir gratuitement le service de blocage des appels.

Ce désir ou besoin d'anonymité est bien naturel pour les gens qui appellent des lignes ouvertes en cas de crise ou pour les bénévoles qui doivent souvent retourner des appels depuis leur domicile. D'ores et déjà, bien des gens - des psychiatres aux agents de probation et des policiers aux policiers en civil - risquent de ne plus pouvoir téléphoner de chez eux, de peur que leur numéro de téléphone ne soit affiché et pris en note. En outre, bien des gens s'inquiètent de l'utilisation commerciale qu'on pourrait faire de leur numéro de téléphone. Quiconque appelle une entreprise s'expose désormais à voir son numéro de téléphone pris en note, puis à être rappelé dans le contexte de campagnes de démarchage. De plus, grâce aux bottins téléphoniques inversés (dans lesquels les abonnés sont inscrits dans l'ordre de leurs numéros de téléphone) on peut facilement trouver les noms et les adresses.

C'est payer bien cher les quelques avantages du SGA que d'y sacrifier la vie privée de tous les usagers. De plus, facturer les abonnés pour **prévenir** l'affichage de leurs numéros, signifie que la protection de la vie privée est à vendre, et certains n'auront pas les moyens de s'offrir ce luxe.

Les appareils de télécommunication : c'est jouer avec la vie privée

Les lecteurs assidus des rapports annuels se rappellent peut-être que l'ancien Commissaire à la protection de la vie privée s'inquiétait des dangers de la nouvelle technologie des télécommunications pour la vie privée (Rapport annuel 1989-1990, p. 32). Le Commissaire s'inquiétait particulièrement du nouveau Service de gestion des appels (SGA) de Bell Canada, et plus particulièrement de l'Afficheur. Le CRTC a depuis approuvé le service offert par Bell Canada, et la plupart des autres compagnies de téléphone ont maintenant des services analogues.

L'Afficheur n'est qu'un des éléments de la nouvelle technologie téléphonique. Une grande partie des nouveaux services ne sont pas dus à l'amélioration des postes de téléphone, mais bien à la puissance des ordinateurs de commutation. Bien entendu, les usagers ont besoin de téléphones spécialement équipés afin de pouvoir voir et noter le numéro de téléphone affiché avant de décrocher.

Cela peut leur assurer une certaine protection contre les appels de harcèlement. Mais cela s'effectue aussi aux dépens des correspondants, qui ont le droit tout aussi légitime de ne pas souhaiter qu'on connaisse leur numéro de téléphone ou qu'on en prenne note.

● les gouvernements ne devraient pas établir de bases de données génétiques contenant des éléments d'identification ou des banques de matériel génétique pour l'ensemble de la population, aux fins du système de justice pénale.

Le rapport n'est guère qu'un survol du dépistage génétique, mais le Commissaire espère qu'il stimulera la réflexion et l'action avant que de puissants intérêts du secteur public ou du secteur privé ne nous transforment tous, des êtres humains que nous avons toujours été, à la simple somme de nos pièces génétiques.

- les gouvernements devraient limiter l'analyse pathologique de l'ADN dans les enquêtes criminelles aux seules fins d'identification des criminels ou d'exonération des suspects;
- les gouvernements ne devraient pas recueillir de renseignements génétiques personnels portant sur les soins médicaux courants;
- les gouvernements ne devraient pas recueillir de renseignements génétiques personnels portant sur le processus de reproduction;
- les gouvernements ne devraient pas recueillir de renseignements génétiques personnels pour déterminer l'admissibilité des postulants;
- les dispensateurs de services ou de prestations ne devraient pas être autorisés à imposer des tests obligatoires de dépistage génétique pour déterminer si une base absolument volontaire devrait être autorisée; conditions en milieu de travail; seul le dépistage sur génétiques résultant de l'exposition à diverses emplois ou pour identifier des changements chez les employés et chez les candidats postulant des obligations dans le contexte de l'emploi, que ce soit l'imposition de tests de dépistage génétique ou l'interdiction de tests de dépistage génétique;
- les gouvernements, ni le secteur privé ne devraient obliger les gens à connaître leurs traits ou leurs affections génétiques;
- les gouvernements ne devraient recueillir des renseignements génétiques personnels si des dispositions législatives précises les y autorisent;

Les gouvernements seront peut-être tentés de surmonter de graves appréhensions d'ordre éthique pour appliquer les connaissances acquises en génétique afin de favoriser l'eugénisme. Chose certaine, le monde d'aujourd'hui n'est pas exempt de pressions de ceux qui préconisent une société « optimisée ». Dans le secteur privé, la génétique pourrait être utilisée comme moyen d'identification des personnes génétiquement « inférieures ». Pour les infortunées classées dans ce « sous-ordre », l'accès à l'emploi ou aux services risquerait d'être sérieusement réduit.

Autant dans le secteur public que dans le secteur privé, des caractéristiques génétiques indépendantes de notre volonté deviendraient des facteurs déterminants de la façon dont on nous permettrait de vivre notre vie, sans beaucoup d'égards pour les êtres humains que nous sommes tous, au-delà de nos gènes.

Le Commissariat a été effaré par les possibilités de prolifération du nombre et des types d'intrusions rendus possibles par les progrès de la technologie génétique. Par conséquent, il s'est prononcé dans son rapport contre le dépistage génétique obligatoire (et, dans certains cas, volontaire) dans plusieurs situations. Il a aussi pressé le gouvernement fédéral d'étudier l'étendue du dépistage génétique au Canada ainsi que les utilisations futures les plus probables de cette technologie.

Le rapport contient plusieurs recommandations expresses, à savoir :

- chacun devrait raisonnablement être en droit de s'attendre à ce que son patrimoine génétique soit gardé secret;

Cette année, le Commissariat a publié *Le dépistage génétique et la vie privée*, troisième volet de sa trilogie sur le dépistage biomédical (les deux premiers portaient l'un sur le dépistage du VIH et du SIDA et l'autre sur le dépistage antidrogue). Le troisième rapport est un examen des questions découlant du développement rapide de la technologie du dépistage génétique, et notamment de plusieurs de ses utilisations actuelles ou potentielles. Les tests de dépistage pourraient être conçus de façon à sélectionner des employés génétiquement optimaux ou à contrôler les effets des dangers pour leur santé auxquels ils sont exposés en milieu de travail, à déterminer l'admissibilité à des prestations ou à des services comme l'assurance, à diagnostiquer ou à prédire des troubles dans le cours normal de soins médicaux de routine ou de la reproduction humaine (dépistage préconception, prénatal et néonatal) et à permettre aux médecins légistes de produire des éléments de preuve plus précis. Au Canada, le dépistage génétique semble jusqu'à présent avoir été limité à trois domaines : les techniques de reproduction humaine, les soins médicaux courants et les procédures médico-légales. Toutefois, la mise au point de tests moins coûteux et générant plus de renseignements renforcera presque à coup sûr l'intérêt pour ce genre de dépistage. Et les gouvernements ne seront pas les seuls à s'immiscer dans notre vie privée; dans le secteur privé, les employeurs et les assureurs, par exemple, seront de plus en plus séduits par les prétendus avantages d'un dépistage génétique capable de les aider à devancer la concurrence.

Il est facile d'oublier les implications, pour la protection de la vie privée, de technologies que bien d'entre nous ne comprenons pas encore parfaitement. À cet égard, rien n'est aussi dangereux que le dépistage génétique.

Les progrès de la technologie génétique nous permettront certainement d'éliminer des mystères médicaux et, ainsi, de prévenir de nombreuses maladies et d'en traiter efficacement bien d'autres. La technologie nous a déjà permis d'identifier de nombreux traits ou désordres génétiques et parfois même de prédire exactement notre avenir génétique. Ce sont de bonnes nouvelles, mais toute médaille a son revers. En effet, les gènes peuvent révéler des secrets bien gardés sur nos caractéristiques physiques et psychologiques, et ces secrets, nous ne voulons peut-être pas que d'autres les connaissent, même si nous voulons les connaître nous-mêmes! Réduire l'essence même de l'humanité à l'échec au complice des molécules d'ADN (autrefois dit à la structure même de nos gènes), c'est une attaque contre notre intimité que bien peu d'entre nous sommes prêts à tolérer.

Les gouvernements - ou qui que ce soit d'autre - ont-ils le droit de recueillir des renseignements génétiques personnels «dans l'intérêt public» avec ou sans notre consentement? Devrions-nous avoir le droit de protéger nos gènes des inspecteurs de l'État ou du secteur privé?

La doctrine du refus de confirmer l'existence de renseignements quelconques ou de la nier est profondément ancrée dans la mentalité des organismes canadiens oeuvrant dans les secteurs de la sécurité et de la police; l'article 16 nous semble en être le corollaire juridique. Si désagréable que cette doctrine soit dans une société libre et démocratique, il peut être nécessaire que nous la tolérions, dans l'intérêt public. Néanmoins, invoquer cet article en même temps qu'une disposition d'exception quelconque, sauf celle qui porte sur les activités des forces de sécurité et des forces policières (articles 21 et 22), c'est de toute évidence porter une atteinte inacceptable à un droit d'accès déjà trop limité et trop fragile. La Loi devrait être modifiée afin de limiter cette autorité à la sécurité nationale et aux enquêtes criminelles.

Nos droits à l'intimité sont d'autant plus menacés que, même si le Commissaire à la protection de la vie privée peut instruire des plaintes fondées sur cet article, il lui est interdit de divulguer les renseignements obtenus au cours de son enquête, voire de faire état de l'existence des renseignements personnels demandés;

Si le Commissaire ne peut résoudre la plainte, il plonge dans l'absurde. Le seul fait de renvoyer l'affaire à la Cour fédérale l'expose à risquer de révéler l'existence des renseignements et, par conséquent, d'enfreindre sa propre Loi. Bref, il faut ajouter à la Loi un mécanisme permettant au Commissaire en dernier recours de renvoyer ces plaintes aux tribunaux.

La portée de cette exception explique pourquoi le Commissaire accueille avec quelque réticence les ajouts à la liste des organismes d'enquête. Au cours de l'année, on l'a informé qu'on envisageait la création de trois nouveaux organismes de ce genre. Loin de nous l'idée de chercher noise aux organismes en question; c'est plutôt avec la notion même d'un organisme d'enquête que nous avons maille à partir. Les autres exceptions donnent aux responsables des institutions toute la latitude dont ils ont besoin, à condition qu'ils tiennent compte du risque de porter préjudice aux intéressés. Pour le moment, le Commissariat participe aux travaux d'un groupe d'étude qui analyse cette exception, son utilisation et quelques possibilités de rechange pour l'avenir.

L'absurde érigé en système

La Loi a une dernière lacune qu'il faut dénoncer dans ce rapport.

C'est l'article 16, qui permet aux institutions fédérales de refuser de confirmer ou de nier l'existence de renseignements personnels demandés. Pour la plupart d'entre nous, les exceptions à la règle limitent bien assez le droit général d'accès à l'information. Or, l'article 16 va beaucoup plus loin qu'autoriser un simple refus de communiquer des renseignements personnels.

En fait, on n'a généralement pas abusé de cette exception. Par exemple, alors qu'on pourrait s'attendre à ce que la GRC l'invoque souvent, elle ne le fait que rarement, préférant se fonder sur d'autres dispositions de la Loi. Néanmoins, certains cas ont clairement révélé comment l'alinéa peut être mal appliqué.

En voici un exemple frappant. Le directeur des Enquêtes et Recherches de Consommation et Affaires commerciales Canada avait enquête sur une plainte dans laquelle on avait accusé la Tribune de la presse du Parlement d'avoir violé les règles fédérales sur la concurrence en rejetant une demande d'adhésion. L'enquête du ministre n'a révélé aucune violation des règles établies, mais lorsque le plaignant a poursuivi sa démarche en invoquant la Loi pour obtenir copie des opinions exprimées par les membres de la Tribune sur sa demande, le ministre a refusé de les lui communiquer, en vertu de l'alinéa 22(1)a). Étant donné que l'enquête avait été exhaustive, le Commissaire s'est dit d'avis qu'il n'y avait aucune raison valide pour que la demande d'information ait été rejetée. Néanmoins, le ministre n'a rien voulu entendre et le Commissaire n'a rien pu faire de plus, puisque le ministre avait parfaitement le droit de refuser d'obtempérer en se prévalant de la Loi.

C'est ce genre d'exception «générale» qu'il faudrait abroger, car elle s'est révélée inutile même dans des situations aussi délicates que celles d'enquêtes policières. Sous sa forme actuelle, l'alinéa 22(1)a) est simplement une échappatoire commode pour des bureaucrates non désireux de se donner la peine de justifier leurs décisions. Par contre, l'alinéa 22(1)b), qui impose comme condition de refus de communiquer les renseignements que leur divulgation risque d'avoir des conséquences néfastes, pose un principe raisonnable permettant aux institutions gouvernementales de gérer efficacement leurs programmes.

Néanmoins, certaines exceptions vont peut-être trop loin. Ainsi, en vertu de l'article 19, de l'alinéa 22(1)a) et du paragraphe 22(2), les organismes gouvernementaux peuvent - ou doivent - refuser de communiquer des renseignements personnels sans être tenus de démontrer que cette communication risquerait de porter préjudice à quelqu'un. Ces trois dispositions visent respectivement les renseignements personnels obtenus d'autres gouvernements, ceux qui sont utilisés pour des activités destinées à faire respecter les lois et enfin ceux qui ont été obtenus par la GRC dans l'exercice de fonctions de police provinciale ou municipale. Les renseignements personnels protégés par le secret professionnel qui lie un avocat à son client (article 27) font eux aussi l'objet d'une exception analogue.

L'alinéa 22(1)a) est certainement l'aspect le plus choquant car il autorise le gouvernement à refuser l'accès à des renseignements personnels préparés au cours d'enquêtes illicites ayant trait aux activités destinées à faire respecter les lois fédérales ou provinciales», à condition que l'enquête soit menée par un «organisme d'enquête». Il y a neuf organismes d'enquête énumérés dans la réglementation découlant de la Loi sur la protection des renseignements personnels. Autrement dit, cette exception équivaut à donner carte blanche à ces organismes, qui peuvent refuser de donner l'accès aux Canadiens à des renseignements personnels qui les concernent, pour toutes les raisons imaginables, voire sans raison. Aucun organisme ne devrait avoir le droit de refuser cet accès sans justification.

La Loi sur la protection des renseignements personnels donne aux Canadiens une liste impressionnante de droits d'accès à des renseignements, mais elle donne aussi aux institutions gouvernementales un arsenal, que d'aucuns qualifieraient cyniquement d'inépuisable, de dispositions d'exception qui leur permettent d'en faire fi. Ces exceptions-là ne sont pas déraisonnables si elles peuvent être étayées par un raisonnement clair et logique, et c'est le cas, la plupart du temps. Ainsi, qui voudrait que des terroristes n'aient qu'à demander à consulter les documents personnels qui les concernent pour savoir que la police est sur le point de leur mettre la main au collet?

Elargissement du critère du préjudice causé aux personnes concernées

Il est vrai que, dans les enquêtes concernant la sécurité nationale ou des procédures pénales, il n'est peut-être pas possible ou avisé de prévenir les individus concernés avant de communiquer ce genre de renseignements personnels. Toutefois, dans ces cas-là, la communication peut être étayée de pièces justificatives, afin que le Commissaire à la protection de la vie privée puisse juger si elle est justifiée.

Il est vrai que, dans les enquêtes concernant la sécurité nationale ou des procédures pénales, il n'est peut-être pas possible ou avisé de prévenir les individus concernés avant de communiquer ce genre de renseignements personnels. Toutefois, dans ces cas-là, la communication peut être étayée de pièces justificatives, afin que le Commissaire à la protection de la vie privée puisse juger si elle est justifiée.

Est-ce que les renseignements personnels ne méritent pas d'être au moins aussi bien protégés contre les divulgations abusives que les renseignements commerciaux?

analogue aux individus quand des renseignements personnels sont communiqués. La Loi sur la protection des renseignements personnels, elle, ne reconnaît pas de droit d'information. La Loi sur la protection des renseignements personnels prévoit un mécanisme servant à alerter les tiers - des compagnies, par exemple - quand des renseignements commerciaux délicats qui les concernent peuvent faire l'objet d'un échange d'information.

Cette façon de procéder pourrait aussi éliminer une autre difficulté inhérente à la communication pour des usages compatibles avec les fins auxquelles les renseignements ont été recueillis. En effet, le paragraphe 9(1) de la Loi impose aux organismes fédéraux l'obligation d'aviser le Commissaire à la protection de la vie privée des cas où ils vont communiquer des renseignements personnels à des fins «compatibles» lorsque celles-ci ne figurent pas parmi celles énumérées dans *Info Source*. Or, le Commissariat n'a reçu et évalué que 18 avis de ce genre depuis sa création. L'expérience acquise grâce à l'instruction des plaintes et aux vérifications lui a appris qu'il y a régulièrement des communications à des fins «compatibles» sans que le Commissaire en soit avisé, comme il se doit. Si les plus hautes instances des organismes étaient tenues de rendre des comptes à ce sujet, la Loi serait respectée plus intégralement et avec plus de diligence.

Le Commissaire souhaite une amélioration des articles 7 et 8, mais il reste que la principale lacune du code des pratiques d'information équitables est qu'il ne prévoit aucun moyen pour un individu d'empêcher la communication de renseignements personnels qui le concernent avant qu'on ait pu juger de sa pertinence. Comme nous l'avons déjà précisé dans plusieurs rapports annuels, il est paradoxal que les gens à qui on refuse l'accès aux renseignements personnels qui les concernent puissent en appeler de cette décision devant les tribunaux, sans toutefois pouvoir en appeler de la décision d'un ministre ou d'un organisme de communiquer ces mêmes renseignements personnels à des tiers.

Chose curieuse, l'un des points forts de la loi est précisément la communication de renseignements pour des raisons d'intérêt public. La loi n'interdit pas ces communications-là et ne tente pas non plus de substituer des règles écrites détaillées au jugement réfléchi du responsable de l'institution. Elle établit simplement des principes d'une transparence manifeste garantissant que toutes les parties intéressées soient dûment informées et que le responsable exerce convenablement la latitude dont il dispose pour la communication des renseignements personnels. C'est le responsable de l'institution après tout, qui connaît le mieux ses documents; c'est donc à lui de concilier l'intérêt du public et le préjudice qu'il risque de faire subir à l'individu concerné.

Il reste que la plupart des communications sans consentement ne forcent pas le responsable de l'institution à se prévaloir de cette latitude, car il peut dans bien des cas déléguer la décision à son personnel. À cet égard, cet alignement est perfectible. En effet, il ne faudrait pas qu'on délègue au personnel le pouvoir de communiquer des renseignements personnels pour des usages compatibles avec les fins auxquelles ils ont été recueillis ou préparés, pour les échanges d'information avec le gouvernement d'une province ou d'un État étranger ou pour la communication de renseignements à des organismes d'enquête, à des députés fédéraux, des chercheurs, des vérificateurs ou des associations d'autorités. Étant donné qu'il s'agit dans ces cas-là de dérogations importantes au principe du consentement préalable de l'individu concerné, c'est le responsable de l'institution lui-même qui devrait être tenu de décider si la communication est justifiée.

Certains prétendront que cette modification revient à modifier inutilement une définition déjà élégante. Pourtant, les données génétiques présentent de tels risques pour notre intimité qu'il est tout à fait justifié qu'elles soient mentionnées expressément dans la Loi.

Resserrement des conditions sur la communication des renseignements personnels

La protection des renseignements personnels repose sur les articles 7 et 8 de la Loi. Le principe fondamental à respecter est celui du consentement en connaissance de cause de l'individu concerné.

Autrement dit, il est interdit d'utiliser ou de communiquer des renseignements personnels sans que l'individu concerné en soit informé et qu'il y consente.

La Loi sur la protection des renseignements personnels confirme une fois de plus que les règles doivent souvent tolérer des exceptions. Ces exceptions sont nécessaires pour concilier le droit de l'individu à la confidentialité des renseignements personnels le concernant et la responsabilité du gouvernement de gérer les affaires de l'État. Ainsi, il est raisonnable que des renseignements personnels soient divulgués sans le consentement de l'individu concerné pour satisfaire à des exigences juridiques ou pour qu'on puisse mener une enquête dans une procédure pénale.

Une nouvelle définition des « renseignements personnels »

Les architectes de la Loi sur la protection des renseignements personnels ne pouvaient pas prévoir l'émergence des techniques d'aujourd'hui quand ils ont proposé leur définition des renseignements personnels. Or, les progrès de la génétique, par exemple, confèrent un sens bien plus vaste à « des renseignements, quels que soient leur forme et leur support, concernant un individu identifiable » [définition des renseignements personnels, à l'article 3 de la Loi].

En effet, même la plus petite gouttelette de liquide ou le plus infime fragment de tissu tiré du corps d'un être humain recèle une masse de renseignements qui définissent avec des détails effarants les traits non seulement de l'individu lui-même, mais aussi ceux de ses ancêtres. Or, même si les alinéas 3b) et 3d) de la Loi portent sur les renseignements relatifs aux dossiers médicaux et aux groupes sanguins, il n'est pas clair que les renseignements concernant un individu identifiable qui sont contenus dans des prélèvements biologiques tombent sous le coup de l'article 3. Bien sûr, le Commissariat compte maintenir mordicus que oui, mais il suffirait de modifier l'article 3 en ce sens pour tuer dans l'oeuf toute controverse à ce sujet. En somme, nous recommandons qu'on reconnaisse clairement dans la définition donnée par la Loi que les renseignements contenus dans un échantillon génétique sont bel et bien des renseignements personnels aux fins de l'application de la Loi.

La principale lacune de la Loi est qu'elle ne s'applique qu'aux renseignements détenus par le gouvernement du Canada et par certains de ses organismes. Les pratiques d'information équitables qu'elle prévoit n'ont été reprises dans leurs propres lois que par quelques autres gouvernements seulement, et pas par le secteur privé, à quelques rares exceptions près. Nous pouvons donc affirmer que la plus grande partie - et de loin - des renseignements personnels détenus par des organismes et des entreprises canadiennes n'est toujours pas protégée.

À moins de réformes, la *Loi sur la protection des renseignements personnels* continuera d'être le plus important texte législatif du pays dans ce domaine, aussi bien parce que le gouvernement du Canada détient une masse énorme de renseignements personnels que parce qu'elle est l'étalon auquel les normes de protection des renseignements détenus dans d'autres secteurs peuvent être mesurées.

Bref, s'il est vrai que la Loi a une bonne fiche, il reste qu'elle doit constamment être réévaluée, non pas pour être modifiée de fond en comble, mais plutôt pour être «bonifiée», dans le jargon à la mode. Le Parlement l'a déjà soumise à un examen en 1986-1987, conformément au paragraphe 75(1). Mais six ans se sont écoulés depuis et le moment est peut-être venu de faire un autre examen.

Etonnamment, nous recommandons de renforcer les points forts de la Loi, c'est-à-dire la définition des renseignements personnels (article 3), le code des pratiques d'information équitables (articles 4 à 8) et la procédure d'accès aux renseignements personnels (articles 12 à 28).

La Loi sur la protection des renseignements personnels est en vigueur depuis maintenant neuf ans; soit depuis assez longtemps pour que des observateurs puissent poser des jugements provisoires sur son efficacité. Eh bien! Elle mérite de bonnes notes.

Une loi parfaite

ne justifiaient pas les moyens intrusifs nécessaires. Ce qui s'est passé au cours de la dernière année nous laisse entendre que le moment est venu de chercher des moyens d'assurer le respect du droit individuel à l'intimité dans des secteurs d'activité où il y a des problèmes particuliers de sécurité ou d'une autre nature. Qu'on ne s'y trompe pas : le Commissaire ne prétend pas qu'on ne pourra jamais justifier un programme de dépistage, mais bien que, pour être acceptable, ces programmes doivent manifestement répondre à un besoin et être efficaces.

La doctrine des pratiques d'information équitables qui sous-tend la *Loi* s'est adaptée à des situations très variées dans un environnement en rapide évolution, et tout indique qu'elle sera vraiment durable. Chose certaine, on n'est pas encore arrivé à concevoir de meilleurs principes.

La protection de la vie privée en milieu de travail est elle aussi une question de plus en plus préoccupante, comme en témoigne la décision prise cette année par deux grandes compagnies (la Banque Toronto-Dominion et Exxon Canada) de mettre sur pied des programmes de dépistage des drogues. Dans les études déjà réalisées à ce sujet, le Commissariat a insisté sur l'utilité très limitée des programmes de ce genre, en concluant que les résultats susceptibles d'être obtenus

La protection de la vie privée en milieu de travail

Le Commissaire appuie avec enthousiasme la démarche de l'ACNOR à qui il a promis l'appui du Commissariat. Les organismes du secteur privé qui cherchent des solutions pratiques aux problèmes de la protection de la vie privée pourraient bien découvrir que l'approche de l'ACNOR est précisément celle qu'ils recherchaient.

Au besoin, l'ACNOR embauchera un expert-conseil d'expérience qui fera des recherches et poursuivra l'élaboration du code avec l'aide du comité. Adopté par consensus, ce code sera la pierre angulaire, étayée par diverses normes techniques, d'un système national qui aidera les différents secteurs d'activité à se doter des codes de protection de la vie privée adaptés à leurs besoins particuliers.

Le comité d'établissement du code de l'ACNOR (sur lequel le Commissariat est représenté) a rédigé une proposition qui lui a déjà valu des déclarations d'intérêt et des subventions d'AMEX, de Readers' Digest, de Bell Canada, d'Equifax et des ministères fédéraux Consommation et Affaires commerciales Canada ainsi que des Communications.

Peu de temps après que le Commissaire eut parlé du projet de directive européenne sur la protection des données personnelles dans son dernier rapport annuel, l'ACNOR a communiqué avec le Commissariat pour lui faire la proposition suivante : mettre sur pied un comité chargé d'élaborer un code modèle de protection des renseignements personnels, code qui pourrait servir de norme nationale minimale pour les organismes du secteur privé qui traitent des renseignements personnels.

L'ACNOR est l'organisme idéal pour développer un tel code. Organisme de service indépendant, il est composé de représentants des gens d'affaires, de l'industrie privée, des syndicats, des universités et des organismes de réglementation. La proposition de l'ACNOR est un prolongement naturel de ses activités de normalisation de la technologie internationale et de son intérêt pour l'impact de la technologie sur les consommateurs, les entreprises et l'industrie privée.

L'adoption d'un code modèle de pratique pour le secteur privé nous donnerait un moyen de concilier les intérêts commerciaux et le droit inhérent des consommateurs à l'intimité. Par ailleurs, l'établissement d'un code confirmerait l'engagement des entreprises canadiennes à respecter les principes de protection de la vie privée énoncés dans les lignes directrices de l'OCDE, et donc de satisfaire à la condition posée par la Communauté européenne qui exige une protection équivalente ou adéquate.

Au moment d'aller sous presse, et pour des raisons que nous avons déjà mentionnées, ces mesures encouragées bien qu'imparfaites pourraient avoir été supplantées par un règlement adopté en vertu de la nouvelle *Loi sur les banques*. Si c'était le cas, cela serait l'amorce d'une importante collaboration entre les autorités gouvernementales et celles du secteur privé. D'un autre côté, si ce n'était pas le cas, le Commissaire demeure convaincu que, bien qu'il faille féliciter les banques pour les progrès qu'elles ont réalisés jusqu'à présent, leurs codes manquent toujours de vigueur.

Nous nous devons aussi de répéter qu'il y a des signes de progrès encourageants dans le secteur du marketing direct, qui a fait l'objet ces dernières années de bien des préoccupations et de nombreuses plaintes du public. Le Commissaire a déjà applaudi la décision de l'Association canadienne du marketing direct (ACMD) de créer un système grâce auquel les Canadiens pourraient faire rayer leurs noms des listes que détiennent les compagnies qui en sont membres. Depuis, l'ACMD a continué à élaborer un code élargi. Ce code n'est pas encore publié, mais le Commissaire espère ardemment qu'il donnera aux consommateurs un rôle beaucoup plus important à jouer, au moins dans la mesure où il sera interdit d'inscrire leur nom sur des listes de ce genre sans leur consentement.

Signalons aussi une autre initiative prometteuse prise au cours de l'année, celle-là par l'Association canadienne de normalisation (ACNOR), qui a pour principale responsabilité d'assurer la sécurité et la fiabilité des produits mis en marché au Canada. Son logo (CSA), qu'on retrouve sur les produits conformes aux normes de l'entreprise privée, est bien connu des Canadiens.

Le secteur privé : une réglementation volontaire

Tous ces faits nouveaux sont très positifs, car ils prouvent bien que nos élus reconnaissent de plus en plus la protection de la vie privée non seulement comme un droit pour chacun de nous, mais aussi comme un droit qu'il faut étayer par des lois et des règlements pour le défendre contre une technologie de plus en plus intrusive.

L'introduction d'une protection de la vie privée dans la troisième province la plus peuplée du Canada signifie que plus de 60 pourcent des Canadiens bénéficieront bientôt d'un service provincial de défense de leur intimité, (les Québécois et les Ontariens en ayant déjà un). Le Commissaire est heureux de pouvoir dire qu'il a eu des discussions avec les autorités d'une autre province où l'on envisage aussi l'adoption d'une loi analogue.

Comme nous l'avons mentionné auparavant, une grande partie du secteur bancaire canadien est désormais volontairement régie par des codes de protection de la vie privée. L'Association des banquiers canadiens a amorcé cette démarche en promulguant un modèle de code, et plusieurs des plus importantes banques à chartre en ont adopté un par la suite. Les détails de ces codes diffèrent, et aucun n'est idéal, mais ils se ressemblent tous sur un point important : ils reconnaissent que le sort réservé aux renseignements personnels que les clients et consommateurs divulguent aux banques les intéresse, et qu'ils ont le droit à la fois de consentir à ce que les institutions bancaires s'en servent et de contrôler cet usage.

Cela dit, le nouveau projet de loi sur les télécommunications que le Parlement étudie présentement est encore plus explicite : il reconnaît que la protection de la vie privée est l'un de ses objectifs. Hormis la *Loi sur la protection des renseignements personnels*, c'est selon le Commissaire, la première loi connue à contenir une disposition aussi explicite.

Au moment d'aller sous presse, le résultat de ces initiatives n'est pas encore connu. Cependant, le Commissaire se dit content de voir cette preuve d'une compréhension croissante des problèmes de protection de la vie privée aussi bien chez les législateurs que dans l'administration fédérale.

En fait, le Commissaire estime qu'on peut voir là une possibilité de solution - ou à tout le moins l'ébauche d'une solution - au problème si souvent débattu de la régulation des pratiques de traitement des renseignements personnels du secteur privé. Toujours dans le domaine législatif, le Commissaire remarque avec beaucoup de satisfaction la proclamation de la *Loi de la Saskatchewan sur l'accès à l'information et sur la protection des renseignements personnels*, ainsi que de l'intention du gouvernement de la Colombie-Britannique de déposer sous peu un projet de loi analogue. À cette fin, la Colombie-Britannique a retenu les services du professeur F. Murray Rankin comme principal expert-conseil, ce qui l'assure que sa démarche bénéficiera d'un dévouement exceptionnel et de connaissances très étendues.

La protection de la vie privée dans les secteurs des banques et des télécommunications

Au palier fédéral, nous avons peut-être franchi un point de non-retour depuis que figurent dans deux importants projets de loi des dispositions susceptibles de répondre aux préoccupations des partisans de la protection de la vie privée. Le premier de ces projets de loi est la nouvelle version de la *Loi sur les banques* et des textes légaux qui en découlent; il sera désormais possible pour des institutions financières comme les banques d'être propriétaires de compagnies d'assurance et de fiducie, et vice versa. Or, les institutions financières disposent d'une telle masse de renseignements personnels que le Commissariat s'inquiète tout naturellement de la mesure dans laquelle elles pourraient partager ces renseignements, ainsi que du degré de consentement et de contrôle des clients et des consommateurs sur ce genre d'échange d'information.

Le projet de loi donne aux autorités gouvernementales le pouvoir d'adopter des règlements à ce sujet. En avril, le Commissaire a comparu devant le Comité sénatorial des banques pour inviter instamment le Parlement à se prévaloir de ce pouvoir d'adopter des règlements.

Le Comité a manifesté beaucoup d'intérêt pour cette recommandation et déclaré que le Commissaire pourrait être invité à lui en reparler. Le Commissaire d'ailleurs sait que le ministère des Finances se penche lui aussi sur la question.

Malheureusement, la proposition du Commissariat n'a pas été appuyée par la majorité des membres du Comité. Bien entendu, nous ne savons pas exactement de quoi le Comité a discuté à *huit clos*, mais nous avons cru comprendre que certains de ses membres ont dit craindre que l'inclusion d'un droit à l'intimité dans la Constitution risquerait de limiter d'autres droits ou libertés (comme la liberté d'expression ou le droit d'accès à l'information). À cet égard, on devrait souligner qu'un éventuel droit à l'intimité ne devrait être accordé qu'à condition que l'intérêt privé et l'intérêt public soient conciliés, comme pour tous les autres droits et libertés déjà garantis par la *Charte*. En effet, la *Charte* précise que ces droits doivent être exercés de façon raisonnable dans une société libre et démocratique, ce qui impose aux tribunaux le devoir de concilier les prétentions contradictoires ou conflictuelles.

Le sort réservé à cette initiative a été d'autant plus décevant que l'épuisement général qui suivra vraisemblablement la fin de la ronde actuelle de négociations constitutionnelles risque fort d'empêcher pour longtemps toute tentative de modification de la *Charte*. Cela dit, la question reste entière pour le Commissaire, et le Commissariat continuera à faire valoir son point de vue.

La protection de la vie privée par la Charte

L'importance d'un public bien informé doit en outre être envisagée dans le contexte d'une nation dont la Constitution ne reconnaît toujours pas clairement le droit à l'intimité. Même s'il existe diverses lois comme au fédéral la *Loi sur la protection des renseignements personnels*, qui accordent aux citoyens une certaine protection dans des domaines bien précis de la collecte de renseignements, et même si la Cour suprême a reconnu un droit à l'intimité dans certains arrêts portant essentiellement sur des questions de droit pénal, il n'en demeure pas moins que l'acceptation du droit à l'intimité comme droit fondamental de la personne n'a toujours pas été entériné dans les lois du pays.

Le Commissariat a tenté d'y remédier, en présentant au Comité spécial mixte sur le renouvellement de la Constitution du Canada une communication dans laquelle il l'a pressé d'inclure le droit à la protection de la vie privée dans ses recommandations.

Dans ce document, le Commissaire a souligné que le droit à l'intimité figurait dans ce qui était presque la toute première ébauche de la *Charte des droits et libertés* et qu'il fait déjà partie intégrante de plusieurs documents analogues, tels que la *Charte des droits de Québec*, la *Déclaration universelle des droits de la personne*, la *Convention européenne sur les droits de la personne* et les constitutions de plusieurs états des États-Unis d'Amérique, pour ne citer que quelques-uns de ces documents. De plus, l'idée a été favorablement accueillie par le Comité de la justice de la Chambre des communes (en 1987) et elle a été appuyée par des organismes nationaux importants, comme l'Association du barreau canadien.

les banques et les entreprises de transport. Pour sa part, le Commissaire actuel a toujours cru que ce n'était pas la meilleure, mais peut-être la seule chose à faire, étant donné l'impossibilité manifeste d'assurer autrement une protection efficace de la vie privée dans le secteur privé. L'urgence du problème s'atténue dans une certaine mesure, étant donné que le Parlement étudie les incidences sur la protection de la vie privée des projets de loi que le gouvernement a déposés à l'égard des institutions financières et des télécommunications. Il faudra en attendre les résultats pour savoir si cette approche ponctuelle est la meilleure. C'est d'ailleurs l'approche que les Pays-Bas sont en train d'adopter. Par exemple, dans le cas des banques canadiennes, l'Association des banquiers canadiens elle-même, et plusieurs de ses membres se sont déjà donné des codes de protection de la vie privée qui, une fois améliorés, pourraient fort bien devenir le noyau d'un ensemble de règlements sur la façon des banques de traiter les renseignements personnels. Le principal élément manquant dans les codes actuels est un système indépendant de supervision et de règlement des différends, indispensable pour assurer le respect des règlements et la confiance du public. Quoi qu'il en soit, il est plus urgent de sensibiliser davantage les citoyens et de mieux les informer, car un public bien informé est la meilleure défense contre les abus. C'est aussi vrai pour la protection de la vie privée que pour celle de la démocratie dans son ensemble, et c'est certainement un élément indispensable à toute défense efficace.

L'obligation d'informer les gens vaut autant pour le secteur privé que pour le secteur public. Dans ce secteur, le seul organisme national qui cherche à suivre constamment l'évolution du dossier global de la protection de la vie privée est précisément le Commissariat à la protection de la vie privée, qui est par conséquent le mieux placé pour jouer un rôle de leader dans l'éducation du public et dans les communications à ce sujet. Et pourtant, le Commissariat n'a pas mandat de faire l'éducation du public, bien que même des parlementaires soient étonnés de se le faire dire. Nous faisons ce que nous pouvons avec des ressources quasi inexistantes, grâce essentiellement au rapport annuel, à des discours et à des conférences, quand le temps nous le permet, et grâce aussi aux bons soins des médias, reconnaissons-le.

Aucun de ces facteurs ne doit être négligé, et surtout pas le dernier. Néanmoins, il est possible et souhaitable de faire beaucoup plus. On a peut-être oublié que le gouvernement s'était engagé en 1987 à réviser la *Loi sur la protection des renseignements personnels* afin de doter le Commissariat d'un mandat visant l'éducation, souhaitons que ce rappel fera progresser le dossier.

Au fil des années, le Commissaire et son prédécesseur ont discuté sur l'opportunité d'étendre la portée de la *Loi sur la protection des renseignements personnels* aux organismes privés de compétence fédérale, comme

La réaction du public à l'explosion du marketing direct est un autre indice de l'importance critique d'une meilleure sensibilisation du public à ces questions. Nous ne prétendons pas que les entreprises de marketing direct sont dépourvues du sens des responsabilités, mais il faudrait être naïf pour ne pas reconnaître que c'est l'inquiétude du public quant aux moyens utilisés par ces compagnies pour obtenir leurs renseignements qui les a incitées à se doter d'un meilleur code de protection de la vie privée.

Par conséquent une meilleure compréhension des problèmes de protection de la vie privée par le public, dans le contexte de la technologie moderne, est une absolue nécessité. Existe-t-il un exemple plus simple et plus percutant que l'expérience vécue récemment avec les téléphones cellulaires?

À la lecture de notre dernier rapport annuel, bien des gens semblent avoir été étonnés d'apprendre que les conversations par téléphone cellulaire pouvaient facilement être interceptées avec du matériel facile d'accès. Cette révélation n'a pas réduit l'engouement du public pour des appareils aussi utiles, mais je parierais que bien des gens sont désormais beaucoup plus prudents lorsqu'ils les utilisent.

En fin de compte, dans le dossier du téléphone cellulaire, la seule donnée manquante était de l'information. La couverture que les médias ont accordée à nos observations a largement contribué à y remédier, mais il n'y aurait pas eu de lacune si les compagnies avaient eu l'obligation de veiller à ce que leur clientèle obtienne toute l'information nécessaire pour prendre des décisions judicieuses sur ces appareils.

Amérique du Nord seulement - représente des milliards de dollars. Une société qui accepte sans sourciller que des inconnus possèdent des dossiers à l'exactitude incertaine sur des millions de personnes et ce sans droit d'accès et de correction, c'est une société téméraire par son indifférence à la préservation de l'aspect le plus fondamental de la protection de la vie privée : le droit des gens à un certain contrôle sur ce que les autres savent à leur sujet. Et pourtant, telle est la situation d'aujourd'hui. Nous sommes à peu près tous fichés dans au moins un - et probablement bien plus d'un - des fichiers informatiques des banques de données et autres marchands de listes.

Il s'agit toutefois d'indifférence largement imputable à l'ignorance. De nombreuses preuves manifestes démontrent que, chaque fois que le public comprend clairement la situation et qu'il a la possibilité d'intervenir, des légions de partisans de la protection de la vie privée montent sur les barricades, parfois avec des résultats étonnants.

Par exemple, il y a quelques années, une compagnie de téléphone américaine avait demandé à ses abonnés s'ils s'opposeraient à ce que les renseignements personnels qu'elle détenait sur eux soient vendus à d'autres entreprises. Quand 800 000 abonnés ont dit qu'ils s'y opposeraient, la compagnie a laissé tomber. Et le jour où l'une des grandes entreprises de production de listes des Etats-Unis a avancé l'idée de commercialiser un disque lisible par machine contenant des renseignements sur 80 millions de personnes, l'idée a provoqué une telle controverse qu'elle a été abandonnée, elle aussi.

• Quoique techniquement cela n'ait pas eu lieu cette année, le Conseil canadien de la radiotélévision et des télécommunications a rendu une décision qui fera époque, dans le dossier de «l'Afficheur», en établissant le principe critique que les abonnés qui veulent préserver la confidentialité de leur numéro de téléphone ne devraient pas avoir à payer un supplément à cette fin. Cette décision capitale reconnaît clairement que, dans le domaine des télécommunications, la protection de la vie privée est un droit acquis du consommateur plutôt qu'un simple «produit» à vendre.

Nous reviendrons plus longuement sur certains de ces points dans les pages suivantes. La liste qui précède n'est pas un relevé exhaustif de ce qui s'est produit dans les nombreux secteurs de la vie et du commerce qui ont eu cette année un impact sur la protection de la vie privée; elle ne contient que des exemples d'une tendance encourageante! Néanmoins, pris individuellement ou collectivement, ils sont bien moins que des victoires éclatantes, ces exemples sont certainement bien préférables au statu quo.

Cependant, il reste que tout cela doit être interprété dans un contexte d'une autre envergure. Le fait est que toutes les pressions des partisans de la protection de la vie privée n'ont jusqu'à présent pas eu d'effet sur le problème le plus crucial et le plus fondamental de la protection de la vie privée, à savoir l'énorme trafic des renseignements personnels qui échappe à toute réglementation et dont le chiffre d'affaires - en

• Deux nouvelles provinces, la Colombie-Britannique et la Saskatchewan, sont à se doter d'organismes de protection de la vie privée et une troisième, l'Alberta, envisage de leur emboîter le pas. Quand elles auront toutes trois fait le nécessaire, il y aura des mécanismes de protection des renseignements personnels et de la vie privée dans toutes les provinces du Canada, du Québec à la côte du Pacifique.

• L'activité législative fédérale dans les secteurs des télécommunications et des institutions financières a focalisé intensément l'attention sur les aspects de protection de la vie privée de ces deux secteurs, aussi bien dans l'administration fédérale qu'au Parlement. Certaines des réactions envisagées - à l'étude au moment d'aller sous presse - pourraient permettre une percée dans ce dossier difficile, en assurant une protection accrue de notre intimité dans le secteur privé.

• Certains des principaux intervenants réagissent maintenant de façon plus énergique à la sensibilisation croissante d'un public mécontent de la façon dont le monde des affaires traite les renseignements personnels qu'il détient. À cet égard, les entreprises canadiennes de marketing direct méritent une mention honorable. En effet, s'il est adopté, le code dont elles envisagent de se doter nous donnera au moins l'espoir que ceux d'entre nous qui ne veulent pas recevoir de courrier indésirable ni être sollicités au téléphone par des vendeurs auront un moyen pratique - annoncé à grand renfort de publicité - d'y échapper.

C'est peut-être trop tenter la fortune, mais l'auteur de ces lignes est quand même prêt à mettre sa boule de cristal - et sa réputation - en jeu pour oser dire que le dossier de la protection de la vie privée semble s'améliorer un peu.

Bien sûr, nous sommes encore loin du beau fixe! Les zones sinistrées abondent toujours et les vestiges de nombreuses défaites jonchent le terrain.

Néanmoins, pour paraphraser outrancièrement Churchill, même si nous sommes loin du début de la fin des problèmes, nous sommes peut-être près de la fin du début.

Bref, disons-le clairement, il semble y avoir eu des progrès.

Au cours de l'année à l'étude, un certain nombre d'événements survenus dans plusieurs secteurs laissent entendre que les forces de la protection de la vie privée - si lentes à se mobiliser - commencent à se faire sentir. Tant au gouvernement que dans le secteur privé, il y a des signes encourageants d'une sensibilisation accrue aux problèmes de protection de la vie privée, et les gens semblent plus disposés à y chercher remède. Voici quelques-uns des exemples les plus frappants de cette évolution.

renseignements donnée dans le manuel *Info Source* est incorrecte à un quelconque égard;

- la liste donnée dans ce manuel pour chaque ministère ne décrit pas tous les usages qui sont faits des renseignements personnels;

- une institution recueille, conserve, utilise ou élimine des renseignements personnels d'une manière qui contrevient à la *Loi sur la protection des renseignements personnels*.

Les enquêteurs du Commissariat à la protection de la vie privée examinent tous les fichiers (y compris ceux considérés inconsultables), à l'exception des renseignements confidentiels du Conseil privé de la Reine, pour s'assurer que les institutions fédérales se conforment à la Loi.

La Loi confère également au Commissaire à la protection de la vie privée le pouvoir de vérifier la façon dont les institutions fédérales recueillent, utilisent et disposent des renseignements personnels, sans devoir attendre qu'une plainte soit déposée.

La Loi sur la protection des renseignements personnels donne aux individus accès à leurs renseignements personnels détenus par le gouvernement fédéral; protège la vie privée des individus en restreignant le nombre des personnes qui peuvent consulter les renseignements; et donne aux individus un certain contrôle sur la collecte et l'usage des renseignements par le gouvernement.

La Loi énonce les principes des pratiques équitables en matière d'information qui exigent que le gouvernement: ne collecte que les renseignements dont il a besoin pour exécuter ses programmes; recueille les renseignements directement auprès de l'individu concerné, dans la mesure du possible; informe l'individu des fins auxquelles ils sont destinés; conserve les renseignements suffisamment longtemps pour en assurer l'accès aux individus; et veille « dans la mesure du possible » à ce que les renseignements personnels soient exacts et complets.

Toute personne présente au Canada peut déposer une plainte auprès du Commissaire à la protection de la vie privée si:

- elle s'est vu refuser une partie quelconque des renseignements;
- le droit de demander la correction de certains des renseignements contenus dans le fichier ou de les annoter leur est refusé;
- le ministre prend plus de 30 jours initiaux ou des 60 jours maximums pour fournir les renseignements; la description du contenu des fichiers de

Table des matières

1	Mandat
3	Le début de la fin?
10	La protection de la vie privée par la Charte.....
12	La protection de la vie privée dans les secteurs des banques et des télécommunications
14	Le secteur privé : une réglementation volontaire
17	La protection de la vie privée au travail
18	Une loi perfectible.....
20	Une nouvelle définition des "renseignements personnels"
21	Resserrement des conditions sur la commu- cation des renseignements personnels
24	Elargissement du critère du préjudice causé aux personnes concernées
27	Laburde érige en système.....
29	Le dépistage génétique
34	Une année dans les tranchées de la vie privée.....
34	Les appareils de télécommunication : c'est jouer avec la vie privée
34	Et la saga du NAS continue
40	Derniers progrès technologiques
44	Couplage de données
49	La division des plaintes.....
53	Quelques cas
66	Aviser le Commissaire
83	Demandes de renseignements - Le public réagit.....
90	Direction de l'observation
97	Tendances et problèmes.....
98	Contrats accordés à l'extérieur - Qui surveille?
98	Vérification de la cote de crédit des employés
100	Transmission électronique de renseignements personnels
102	Qui surveille l'ordinateur?
104	Evaluations vers le haut.....
108	La gestion intégrée
109	Organigramme
112	

L'honorable John A. Fraser, c.p., c.r., député
Président
Chambre des communes
Ottawa

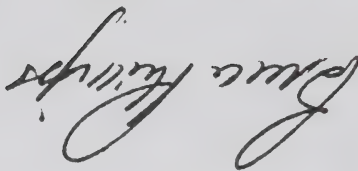
le 12 août 1992

Monsieur Fraser,

J'ai l'honneur de soumettre mon rapport annuel au Parlement.
Ce rapport couvre la période allant du 1^{er} avril 1991 au
31 mars 1992.

Veuillez agréer l'expression de mes sentiments respectueux.

Le Commissaire à la protection de la vie privée



Bruce Phillips

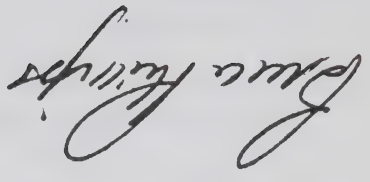
L'honorable Guy Charbonneau
Président
Sénat
Ottawa

le 12 août 1992

Monsieur Charbonneau,
J'ai l'honneur de soumettre mon rapport annuel au Parlement.
Ce rapport couvre la période allant du 1^{er} avril 1991 au
31 mars 1992.

Veuillez agréer l'expression de mes sentiments respectueux.

Le Commissaire à la protection de la vie privée



Bruce Phillips

Page couverture: Les nouvelles "cartes à mémoire" ressemblent à des cartes bancaires ou à des cartes de crédit mais avec une différence importante. Un microprocesseur enchâssé permet le traitement et l'emmagasinement de l'information en plus d'en identifier le propriétaire. Les symboles qui suivent illustrent l'éventail de services et de renseignements personnels qu'on pourrait bientôt retrouver sur un seul petit morceau de plastique. Ceux-ci sont:

- Carte d'appel téléphonique
- Achats au détail
- Laissez-passer
- Dossiers médicaux
- Prestations fédérales
- Services bancaires
- Accès au système informatique
- Accès au domicile et au travail

Le Commissaire à la protection de la vie privée du Canada
112, rue Kent,
Ottawa (Ontario)
K1A 1H3

(613) 995-2410, 1-800-267-0441
Télec. (613) 995-1501
ATS (613) 992-9190

© Ministre des Approvisionnements et Services Canada 1992
N° de cat. IP30-1/1992

ISBN 0-662-59183-6

**Rapport annuel du
Commissaire à la protection de la vie privée
1991-1992**





Commissaire à la protection de la vie privée

Rapport annuel 1991 - 1992

